Commentary on the Directive 2002/58/EC on privacy and electronic communications

DIX, Alexander; Rosier, Karen; Poullet, Yves

Published in:
Concise European IT Law

Publication date:
2006

Document Version
Publisher's PDF, also known as Version of record

DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

(Directive on privacy and electronic communications)

of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector

The European Parliament and the Council of the European Union,

Having regard to the Treaty establishing the European Community, and in particular Article 95 thereof,

Having regard to the proposal from the Commission,[1]

Having regard to the opinion of the Economic and Social Committee,[2]

Having consulted the Committee of the Regions, Acting in accordance with the procedure laid down in Article 251 of the Treaty,[3]

Whereas:

(1) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[4] requires Member States to ensure the rights and freedoms of natural persons with regard to the processing of personal data, and in particular their right to privacy, in order to ensure the free flow of personal data in the Community.

(2) This Directive seeks to respect the fundamental rights and observes the principles recognised in particular by the Charter of fundamental rights of the European Union. In particular, this Directive seeks to ensure full respect for the rights set out in Articles 7 and 8 of that Charter.

(3) Confidentiality of communications is guaranteed in accordance with the international instruments relating to human rights, in particular the European Convention for the Protection of Human Rights and Fundamental Freedoms, and the constitutions of the Member States.

(4) Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector[5] translated the principles set out in

---

1. OJ C 365 E, 19 December 2000, p. 223.
2. OJ C 123, 25 April 2001, p. 53.
3. Opinion of the European Parliament of 13 November 2001 (not yet published in the Official Journal), Council Common Position of 28 January 2002 (OJ C 113 E, 14 May 2002, p. 39) and Decision of the European Parliament of 30 May 2002 (not yet published in the Official Journal). Council Decision of 25 June 2002.
4. OJ L 281, 23 November 1995, p. 31.
5. OJ L 24, 30 January 1998, p. 1.

Directive 95/46/EC into specific rules for the telecommunications sector. Directive 97/66/EC has to be adapted to developments in the markets and technologies for electronic communications services in order to provide an equal level of protection of personal data and privacy for users of publicly available electronic communications services, regardless of the technologies used. That Directive should therefore be repealed and replaced by this Directive.

(5) New advanced digital technologies are currently being introduced in public communications networks in the Community, which give rise to specific requirements concerning the protection of personal data and privacy of the user. The development of the information society is characterised by the introduction of new electronic communications services. Access to digital mobile networks has become available and affordable for a large public. These digital networks have large capacities and possibilities for processing personal data. The successful cross-border development of these services is partly dependent on the confidence of users that their privacy will not be at risk.

(6) The Internet is overturning traditional market structures by providing a common, global infrastructure for the delivery of a wide range of electronic communications services. Publicly available electronic communications services over the Internet open new possibilities for users but also new risks for their personal data and privacy.

(7) In the case of public communications networks, specific legal, regulatory and technical provisions should be made in order to protect fundamental rights and freedoms of natural persons and legitimate interests of legal persons, in particular with regard to the increasing capacity for automated storage and processing of data relating to subscribers and users.

(8) Legal, regulatory and technical provisions adopted by the Member States concerning the protection of personal data, privacy and the legitimate interest of legal persons, in the electronic communication sector, should be harmonised in order to avoid obstacles to the internal market for electronic communication in accordance with Article 14 of the Treaty. Harmonisation should be limited to requirements necessary to guarantee that the promotion and development of new electronic communications services and networks between Member States are not hindered.

(9) The Member States, providers and users concerned, together with the competent Community bodies, should cooperate in introducing and developing the relevant technologies where this is necessary to apply the guarantees provided for by this Directive and taking particular account of the objectives of minimising the processing of personal data and of using anonymous or pseudonymous data where possible.

(10) In the electronic communications sector, Directive 95/46/EC applies in particular to all matters concerning protection of fundamental rights and freedoms, which are not specifically covered by the provisions of this Directive, including the obligations on the controller and the rights of individuals. Directive 95/46/EC applies to non-public communications services.

(11) Like Directive 95/46/EC, this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law. Therefore it does not alter the existing balance between the individual's right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the rulings of the European Court of Human Rights. Such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms.

(12) Subscribers to a publicly available electronic communications service may be natural or legal persons. By supplementing Directive 95/46/EC, this Directive is aimed at protecting the fundamental rights of natural persons and particularly their right to privacy, as well as the legitimate interests of legal persons. This Directive does not entail an obligation for Member States to extend the application of Directive 95/46/EC to the protection of the legitimate interests of legal persons, which is ensured within the framework of the applicable Community and national legislation.

(13) The contractual relation between a subscriber and a service provider may entail a periodic or a one-off payment for the service provided or to be provided. Prepaid cards are also considered as a contract.

(14) Location data may refer to the latitude, longitude and altitude of the user's terminal equipment, to the direction of travel, to the level of accuracy of the location information, to the identification of the network cell in which the terminal equipment is located at a certain point in time and to the time the location information was recorded.

(15) A communication may include any naming, numbering or addressing information provided by the sender of a communication or the user of a connection to carry out the communication. Traffic data may include any translation of this information by the network over which the communication is transmitted for the purpose of carrying out the transmission. Traffic data may, inter alia, consist of data referring to the routing, duration, time or volume of a communication, to the protocol used, to the location of the terminal equipment of the sender or recipient, to the network on which the communication originates or terminates, to the beginning, end or duration of a connection. They may also consist of the format in which the communication is conveyed by the network.

(16) Information that is part of a broadcasting service provided over a public communications network is intended for a potentially unlimited audience and does not constitute a communication in the sense of this Directive. However, in

cases where the individual subscriber or user receiving such information can be identified, for example with video-on-demand services, the information conveyed is covered within the meaning of a communication for the purposes of this Directive.

(17) For the purposes of this Directive, consent of a user or subscriber, regardless of whether the latter is a natural or a legal person, should have the same meaning as the data subject's consent as defined and further specified in Directive 95/46/EC. Consent may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes, including by ticking a box when visiting an Internet website.

(18) Value added services may, for example, consist of advice on least expensive tariff packages, route guidance, traffic information, weather forecasts and tourist information.

(19) The application of certain requirements relating to presentation and restriction of calling and connected line identification and to automatic call forwarding to subscriber lines connected to analogue exchanges should not be made mandatory in specific cases where such application would prove to be technically impossible or would require a disproportionate economic effort. It is important for interested parties to be informed of such cases and the Member States should therefore notify them to the Commission.

(20) Service providers should take appropriate measures to safeguard the security of their services, if necessary in conjunction with the provider of the network, and inform subscribers of any special risks of a breach of the security of the network. Such risks may especially occur for electronic communications services over an open network such as the Internet or analogue mobile telephony.

It is particularly important for subscribers and users of such services to be fully informed by their service provider of the existing security risks which lie outside the scope of possible remedies by the service provider. Service providers who offer publicly available electronic communications services over the Internet should inform users and subscribers of measures they can take to protect the security of their communications for instance by using specific types of software or encryption technologies. The requirement to inform subscribers of particular security risks does not discharge a service provider from the obligation to take, at its own costs, appropriate and immediate measures to remedy any new, unforeseen security risks and restore the normal security level of the service. The provision of information about security risks to the subscriber should be free of charge except for any nominal costs which the subscriber may incur while receiving or collecting the information, for instance by downloading an electronic mail message. Security is appraised in the light of Article 17 of Directive 95/46/EC.

(21) Measures should be taken to prevent unauthorised access to communications in order to protect the confidentiality of communications, including both the contents and any data related to such communications, by means of public communications networks and publicly available electronic communications

services. National legislation in some Member States only prohibits intentional unauthorised access to communications.

(22) The prohibition of storage of communications and the related traffic data by persons other than the users or without their consent is not intended to prohibit any automatic, intermediate and transient storage of this information in so far as this takes place for the sole purpose of carrying out the transmission in the electronic communications network and provided that the information is not stored for any period longer than is necessary for the transmission and for traffic management purposes, and that during the period of storage the confidentiality remains guaranteed. Where this is necessary for making more efficient the onward transmission of any publicly accessible information to other recipients of the service upon their request, this Directive should not prevent such information from being further stored, provided that this information would in any case be accessible to the public without restriction and that any data referring to the individual subscribers or users requesting such information are erased.

(23) Confidentiality of communications should also be ensured in the course of lawful business practice. Where necessary and legally authorised, communications can be recorded for the purpose of providing evidence of a commercial transaction. Directive 95/46/EC applies to such processing. Parties to the communications should be informed prior to the recording about the recording, its purpose and the duration of its storage. The recorded communication should be erased as soon as possible and in any case at the latest by the end of the period during which the transaction can be lawfully challenged.

(24) Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms. So-called spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users. The use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned.

(25) However, such devices, for instance so-called 'cookies', can be a legitimate and useful tool, for example, in analysing the effectiveness of website design and advertising, and in verifying the identity of users engaged in on-line transactions. Where such devices, for instance cookies, are intended for a legitimate purpose, such as to facilitate the provision of information society services, their use should be allowed on condition that users are provided with clear and precise information in accordance with Directive 95/46/EC about the purposes of cookies or similar devices so as to ensure that users are made aware of information being placed on the terminal equipment they are using. Users should have the opportunity to refuse to have a cookie or similar device stored on their terminal equipment. This is particularly important where users other than the original user have access to the terminal equipment and thereby to any data containing privacy-sensitive information stored on such equipment. Information and the right to refuse may be

offered once for the use of various devices to be installed on the user's terminal equipment during the same connection and also covering any further use that may be made of those devices during subsequent connections. The methods for giving information, offering a right to refuse or requesting consent should be made as userfriendly as possible. Access to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose.

(26) The data relating to subscribers processed within electronic communications networks to establish connections and to transmit information contain information on the private life of natural persons and concern the right to respect for their correspondence or concern the legitimate interests of legal persons. Such data may only be stored to the extent that is necessary for the provision of the service for the purpose of billing and for interconnection payments, and for a limited time. Any further processing of such data which the provider of the publicly available electronic communications services may want to perform, for the marketing of electronic communications services or for the provision of value added services, may only be allowed if the subscriber has agreed to this on the basis of accurate and full information given by the provider of the publicly available electronic communications services about the types of further processing it intends to perform and about the subscriber's right not to give or to withdraw his/her consent to such processing. Traffic data used for marketing communications services or for the provision of value added services should also be erased or made anonymous after the provision of the service. Service providers should always keep subscribers informed of the types of data they are processing and the purposes and duration for which this is done.

(27) The exact moment of the completion of the transmission of a communication, after which traffic data should be erased except for billing purposes, may depend on the type of electronic communications service that is provided. For instance for a voice telephony call the transmission will be completed as soon as either of the users terminates the connection. For electronic mail the transmission is completed as soon as the addressee collects the message, typically from the server of his service provider.

(28) The obligation to erase traffic data or to make such data anonymous when it is no longer needed for the purpose of the transmission of a communication does not conflict with such procedures on the Internet as the caching in the domain name system of IP addresses or the caching of IP addresses to physical address bindings or the use of log-in information to control the right of access to networks or services.

(29) The service provider may process traffic data relating to subscribers and users where necessary in individual cases in order to detect technical failure or errors in the transmission of communications. Traffic data necessary for billing purposes may also be processed by the provider in order to detect and stop fraud consisting of unpaid use of the electronic communications service.

(30) Systems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to

a strict minimum. Any activities related to the provision of the electronic communications service that go beyond the transmission of a communication and the billing thereof should be based on aggregated, traffic data that cannot be related to subscribers or users. Where such activities cannot be based on aggregated data, they should be considered as value added services for which the consent of the subscriber is required.

(31) Whether the consent to be obtained for the processing of personal data with a view to providing a particular value added service should be that of the user or of the subscriber, will depend on the data to be processed and on the type of service to be provided and on whether it is technically, procedurally and contractually possible to distinguish the individual using an electronic communications service from the legal or natural person having subscribed to it.

(32) Where the provider of an electronic communications service or of a value added service subcontracts the processing of personal data necessary for the provision of these services to another entity, such subcontracting and subsequent data processing should be in full compliance with the requirements regarding controllers and processors of personal data as set out in Directive 95/46/EC. Where the provision of a value added service requires that traffic or location data are forwarded from an electronic communications service provider to a provider of value added services, the subscribers or users to whom the data are related should also be fully informed of this forwarding before giving their consent for the processing of the data.

(33) The introduction of itemised bills has improved the possibilities for the subscriber to check the accuracy of the fees charged by the service provider but, at the same time, it may jeopardise the privacy of the users of publicly available electronic communications services. Therefore, in order to preserve the privacy of the user, Member States should encourage the development of electronic communication service options such as alternative payment facilities which allow anonymous or strictly private access to publicly available electronic communications services, for example calling cards and facilities for payment by credit card. To the same end, Member States may ask the operators to offer their subscribers a different type of detailed bill in which a certain number of digits of the called number have been deleted.

(34) It is necessary, as regards calling line identification, to protect the right of the calling party to withhold the presentation of the identification of the line from which the call is being made and the right of the called party to reject calls from unidentified lines. There is justification for overriding the elimination of calling line identification presentation in specific cases. Certain subscribers, in particular help lines and similar organisations, have an interest in guaranteeing the anonymity of their callers. It is necessary, as regards connected line identification, to protect the right and the legitimate interest of the called party to withhold the presentation of the identification of the line to which the calling party is actually connected, in particular in the case of forwarded calls. The providers of publicly available electronic communications services should inform their subscribers of the existence of calling and connected line identification in the network

and of all services which are offered on the basis of calling and connected line identification as well as the privacy options which are available. This will allow the subscribers to make an informed choice about the privacy facilities they may want to use. The privacy options which are offered on a per-line basis do not necessarily have to be available as an automatic network service but may be obtainable through a simple request to the provider of the publicly available electronic communications service.

(35) In digital mobile networks, location data giving the geographic position of the terminal equipment of the mobile user are processed to enable the transmission of communications. Such data are traffic data covered by Article 6 of this Directive. However, in addition, digital mobile networks may have the capacity to process location data which are more precise than is necessary for the transmission of communications and which are used for the provision of value added services such as services providing individualised traffic information and guidance to drivers. The processing of such data for value added services should only be allowed where subscribers have given their consent. Even in cases where subscribers have given their consent, they should have a simple means to temporarily deny the processing of location data, free of charge.

(36) Member States may restrict the users' and subscribers' rights to privacy with regard to calling line identification where this is necessary to trace nuisance calls and with regard to calling line identification and location data where this is necessary to allow emergency services to carry out their tasks as effectively as possible. For these purposes, Member States may adopt specific provisions to entitle providers of electronic communications services to provide access to calling line identification and location data without the prior consent of the users or subscribers concerned.

(37) Safeguards should be provided for subscribers against the nuisance which may be caused by automatic call forwarding by others. Moreover, in such cases, it must be possible for subscribers to stop the forwarded calls being passed on to their terminals by simple request to the provider of the publicly available electronic communications service.

(38) Directories of subscribers to electronic communications services are widely distributed and public. The right to privacy of natural persons and the legitimate interest of legal persons require that subscribers are able to determine whether their personal data are published in a directory and if so, which. Providers of public directories should inform the subscribers to be included in such directories of the purposes of the directory and of any particular usage which may be made of electronic versions of public directories especially through search functions embedded in the software, such as reverse search functions enabling users of the directory to discover the name and address of the subscriber on the basis of a telephone number only.

(39) The obligation to inform subscribers of the purpose(s) of public directories in which their personal data are to be included should be imposed on the party collecting the data for such inclusion. Where the data may be transmitted to one or more third parties, the subscriber should be informed of this possibility and of the recipient or the categories of possible recipients. Any transmission should be subject to the condition that the data may not be used for other purposes than those for which they were collected. If the party collecting the data from the subscriber or any third party to whom the data have been transmitted wishes to use the data for an additional purpose, the renewed consent of the subscriber is to be obtained either by the initial party collecting the data or by the third party to whom the data have been transmitted.

(40) Safeguards should be provided for subscribers against intrusion of their privacy by unsolicited communications for direct marketing purposes in particular by means of automated calling machines, telefaxes, and e-mails, including SMS messages. These forms of unsolicited commercial communications may on the one hand be relatively easy and cheap to send and on the other may impose a burden and/or cost on the recipient. Moreover, in some cases their volume may also cause difficulties for electronic communications networks and terminal equipment. For such forms of unsolicited communications for direct marketing, it is justified to require that prior explicit consent of the recipients is obtained before such communications are addressed to them. The single market requires a harmonised approach to ensure simple, Community-wide rules for businesses and users.

(41) Within the context of an existing customer relationship, it is reasonable to allow the use of electronic contact details for the offering of similar products or services, but only by the same company that has obtained the electronic contact details in accordance with Directive 95/46/EC. When electronic contact details are obtained, the customer should be informed about their further use for direct marketing in a clear and distinct manner, and be given the opportunity to refuse such usage. This opportunity should continue to be offered with each subsequent direct marketing message, free of charge, except for any costs for the transmission of this refusal.

(42) Other forms of direct marketing that are more costly for the sender and impose no financial costs on subscribers and users, such as person-to-person voice telephony calls, may justify the maintenance of a system giving subscribers or users the possibility to indicate that they do not want to receive such calls. Nevertheless, in order not to decrease existing levels of privacy protection, Member States should be entitled to uphold national systems, only allowing such calls to subscribers and users who have given their prior consent.

(43) To facilitate effective enforcement of Community rules on unsolicited messages for direct marketing, it is necessary to prohibit the use of false identities or false return addresses or numbers while sending unsolicited messages for direct marketing purposes.

(44) Certain electronic mail systems allow subscribers to view the sender and subject line of an electronic mail, and also to delete the message, without having to download the rest of the electronic mail's content or any attachments, thereby reducing costs which could arise from downloading unsolicited electronic mails or attachments. These arrangements may continue to be useful in certain cases as an additional tool to the general obligations established in this Directive.

(45) This Directive is without prejudice to the arrangements which Member States make to protect the legitimate interests of legal persons with regard to unsolicited communications for direct marketing purposes. Where Member States establish an opt-out register for such communications to legal persons, mostly business users, the provisions of Article 7 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market (Directive on electronic commerce)[1] are fully applicable.

(46) The functionalities for the provision of electronic communications services may be integrated in the network or in any part of the terminal equipment of the user, including the software. The protection of the personal data and the privacy of the user of publicly available electronic communications services should be independent of the configuration of the various components necessary to provide the service and of the distribution of the necessary functionalities between these components. Directive 95/46/EC covers any form of processing of personal data regardless of the technology used. The existence of specific rules for electronic communications services alongside general rules for other components necessary for the provision of such services may not facilitate the protection of personal data and privacy in a technologically neutral way. It may therefore be necessary to adopt measures requiring manufacturers of certain types of equipment used for electronic communications services to construct their product in such a way as to incorporate safeguards to ensure that the personal data and privacy of the user and subscriber are protected. The adoption of such measures in accordance with Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity[2] will ensure that the introduction of technical features of electronic communication equipment including software for data protection purposes is harmonised in order to be compatible with the implementation of the internal market.

(47) Where the rights of the users and subscribers are not respected, national legislation should provide for judicial remedies. Penalties should be imposed on any person, whether governed by private or public law, who fails to comply with the national measures taken under this Directive.

(48) It is useful, in the field of application of this Directive, to draw on the experience of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data composed of representatives of the supervisory authorities of the Member States, set up by Article 29 of Directive 95/46/EC.

(49) To facilitate compliance with the provisions of this Directive, certain specific arrangements are needed for processing of data already under way on the date that national implementing legislation pursuant to this Directive enters into force,

1. OJ L 178, 17 July 2000, p. 1.
2. OJ L 91, 7 April 1999, p. 10.

Have adopted this Directive:

[Scope and aim]

Article 1

(1) This Directive harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.

(2) The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.

(3) This Directive shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.

1. Scope and aim (para. 1). The Directive aims at defining principles of protection with regard to the processing of personal data specifically in the electronic communications sector. It is therefore more specific than the Data Protection Directive which governs the processing of personal data regardless of the processing context. The Directive replaces the Old Directive which ruled the processing of personal data in the telecommunication sector. Para. 1 is almost similar to art. 1 para. 1 of the Old Directive. The only innovation in para. 1 lies in the replacement of the term 'telecommunications' by the more technology neutral terms 'electronic communications'. This adaptation reflects the intention of the European legislator, concomitantly with the telecom reform and the adoption of a package of directives in this regard, to broaden the scope of application of the Directive to include clearly new technologies such as internet and electronic mail and to provide an equal level of protection of personal data and privacy for users of publicly available electronic communications services, regardless of the technologies used. However, if the new text removes any doubts as to its application to these new means of communication, there was already a large consensus that the Old Directive applied to internet and electronic mail. The main merit of the Directive is therefore to establish rules specifically dedicated to new services rendered available through the evolution of technologies such as the provision of value added services (see comment on art. 2 (2)(g)).

2. Link with Data Protection Directive (para. 2). (a) Specific regulation. The Directive particularizes and complements the Data Protection Directive.

According to recital 10, the Data Protection Directive will apply in the electronic communication sector to all matters concerning protection of fundamental rights and freedoms, which are not specifically covered by the provisions of the Directive, including the obligations of the controller and the rights of individuals. Consequently, both Directives will be applicable to the processing in the electronic communication sector, the Data Protection Directive being subsidiary to the Directive. **(b) Scope of application.** Because the Directive particularizes the Data Protection Directive, the Directive should only govern data processing within the electronic communication sector to the extent that processing of personal data is involved, just as in the Data Protection Directive. The text of the Directive, however, does not clearly endorse this principle. Indeed, most of provisions of the Directive are expressed with concepts that differ from those of the Data Protection Directive (see comment on art. 2, note 1(a)). It is therefore not always clear whether the exact scope of the provision should be determined only in the light of the definitions provided within the Directive or if it is also necessary to determine the scope of the terms of the Directive in the light of the provisions of the Data Protection Directive. For instance, art. 5(3) seems to relate to the processing of 'information', regardless of whether this information consists of personal data. It is unclear whether this provision should be construed as governing the processing of any kind of data or it concerns only personal data within the meaning given to these terms in the Data Protection Directive. This lack of consistency in the text of the Directive creates some doubts as to a definition of the scope of application of the Directive rationae materiae and rationae personae by reference to the criteria determining the scope of application of the Data Protection Directive. Moreover, it is quite clear that the two directives do not have the same scope of application rationae loci (see comment on art. 3(1)). **(c) Protection of legal persons' interests.** Besides, there is a remarkable difference between the Directive and the Data Protection Directive. Where the Data Protection Directive only governs the processing of personal data relating to individuals, the Directive contains certain provisions affording a protection of the legitimate interests of the subscribers who are legal persons. Recital 12, however, makes clear that the Directive does not entail an obligation for the Member States to extend the application of the Data Protection Directive to the protection of the legitimate interests of legal persons. The Directive does not define the concept of 'legitimate interest' of legal persons. This might lead to significant discrepancies in the Member States national laws implementing the Directive. For instance, some Member States may consider that authorizing, transmitting or sending electronic mail for marketing purposes to legal persons when the legal person did not expressly oppose such sending affords a satisfactory level of protection of their legitimate interests. By contrast, other Member States may consider it necessary to require consent from the legal person prior to sending unsolicited communication.

3. Matters out of scope (para. 3). The activities falling outside the scope of the Treaty establishing the European Community (Third Pillar's activities) also fall outside the scope of the Directive. Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or to take other measures referred to in art. 15(1), if necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) neither does it affect the enforcement of criminal law for any of these purposes and in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the rulings of the European Court of Human Rights.

[Definitions]

Article 2

(1) Save as otherwise provided, the definitions in Directive 95/46/EC and in Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive on electronic communications) shall apply.

(2) The following definitions shall also apply:

(a) 'user' means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service;

(b) 'traffic data' means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;

(c) 'location data' means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;

(d) 'communication' means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information;

(e) 'call' means a connection established by means of a publicly available telephone service allowing two-way communication in real time;

(f) 'consent' by a user or subscriber corresponds to the data subject's consent in Directive 95/46/EC;

(g) 'value added service' means any service which requires the processing of traffic data or location data other than traffic data beyond what is

necessary for the transmission of a communication or the billing thereof;

(h) 'electronic mail' means any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient.

1. Applicability of definitions provided by the Data Protection Directive and by the Framework Directive on electronic communications (para. 1). At the crossroads of data protection and data conveyance, the Directive takes concepts that are typically proper to these two areas. **(a) Definitions provided in the Data Protection Directive.** The reference to the definitions provided by the Data Protection Directive is logical in light of art. 1(1) since the provisions of the Directive are intended to complement and particularize the provisions of the Data Protection Directive's. The definitions provided in art. 2 of the Data Protection Directive relate to key concepts of the application of data protection legislation such as 'personal data', 'processing of personal data', 'controller' or 'processor'. However, the Directive makes rather limited use of these key concepts and more generally relies on specific proper concepts that are not based on these definitions. For instance, the Directive uses the terms 'traffic data' in arts. 6 and 9, 'location data' in art. 9 or 'information' in art. 5(3) which data or information are not necessarily 'personal data' per se. Likewise, the Directive often imposes obligations and restrictions on providers of a public communications network (in arts. 6 and 10) and providers of publicly available electronic communications services (in arts. 6, 8 and 9) without specifying that it only concerns service providers who are 'controllers' according to the Data Protection Directive's definition thereof. **(b) Definitions provided in the Framework Directive on electronic communications.** The reliance on definitions provided in the Framework Directive on electronic communications is essential to understand the territorial, material and personal scopes of application of the Directive. Art. 3 defines the material and territorial scopes of application of the Directive by reference to 'publicly available electronic communications services in public communications networks'. Indeed, the Directive is not related to 'content' services (governed by the e-commerce Directive) but rather to 'transmission' services. *Definition of 'electronic communications service'.* According to art. 2(c) of the Framework Directive on electronic communications, an 'electronic communications service' means 'a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in art. 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks'. For instance, voice telephony services, internet access and electronic mail conveyance are typical electronic communications services. *Definition of 'electronic communications network'.* These terms refer to 'transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed'. *Definition of 'public communications network'.* Art. 2(d) of the Directive on a common framework for electronic communications networks and services defines a 'public communications network' as 'an electronic communications network used wholly or mainly for the provision of publicly available electronic communications services'. According to this definition, the 'public' character of the network depends on the fact that it is used to provide electronic communications services that are 'publicly available'. As to the personal scope of application of the Directive, several provisions impose specific obligations on the provider of publicly available electronic communications services and on the provider of a public communication network, such as arts. 6 and 9. Art. 2(m) of the Framework Directive on electronic communications states that the provision of an electronic communications network implies the establishment, operation, control or making available of such a network.

2. Definitions of Directive (para. 2). (a) Definitions of 'subscriber' and 'user' (para. 2(a)). *Concept of subscriber.* Para. 2(a) indirectly defines the concept of subscriber to which it is often referred in the Directive. Subscribers are persons who pay for a publicly available electronic communications service whether for private or business purpose. Recital 13 specifies that the contractual relationship between a subscriber and a service provider may entail either a periodic or a one-time payment for the service provided or to be provided. Prepaid cards are also considered a contract. As confirmed in recital 12, subscribers may be legal or natural persons, as compared to the users who are always natural persons. *Concept of user.* According to para. 2(a), a user means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service. For instance, the head of a family may sign a contract with an internet access provider to obtain an e-mail account and to access the internet. This account may allow for the creation of several e-mail addresses for other members of the family. In such a case, members of the family are 'users' who benefit from communications services without being the actual service subscriber. Another example of users would be employees who are benefiting from mobile phone services or internet access services based on a subscription taken by their employer. Some provisions of the

Directive afford a protection to both users and subscribers (such as arts. 6 and 9) while others only relate to the subscribers (see art. 13). **(b) Definition of 'traffic data' (para. 2(b)).** The Old Directive made use of these terms without providing a definition for them. The reason for introducing such a definition in the Directive was to be able to distinguish between such data and the location data (see definition of 'location data' under para. 2(c)). Traffic data are defined by reference to the purpose for which they are processed: these are any data processed for the purpose of the conveyance of a communication on an electronic communications network (such as the phone number calling or being called, the e-mail addresses, IP address of the sender and of the receiver, etc.) or for the billing thereof (such as for the duration of the communication, size of the e-mail sent, phone number calling, etc.). They include data supplied by the sender (URL, e-mail address of the recipient, etc.) as well as data generated by the traffic. According to recital 15, 'traffic data may, inter alia, consist of data referring to the routing, duration, time or volume of a communication, to the protocol used, to the location of the terminal equipment of the sender or recipient, to the network on which the communication originates or terminates, to the beginning, end or duration of a connection. They may also consist of the format in which the communication is conveyed by the network'. Traffic data also include data which qualify as 'location data' (see definition of 'location data' of para. 2(c)) when and to the extent these location data are being processed for transmission and billing activities purposes. **(c) Definition of 'location data' (para. 2(c)).** According to para. 2(c), 'location data' are 'any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service'. This definition first requires that, in order to be considered as 'location data', the data should relate to the localization of terminal equipment. The Directive does not provide for a definition of 'terminal equipment'. This term may have various meanings depending on the context in which it is used. In data communication, the term generally applies to a device that terminates one end, the sender's or receiver's, of a communication. Terminal equipment targeted by the Directive are typically telephone or Global Positioning System (GPS) devices, for instance. The terminal equipment must then belong to a user of publicly available communications services (see definition under comment on para. 1). Location data will therefore always be data processed in an electronic communications network. According to recital 14, 'location data may refer to the latitude, longitude and altitude of the user's terminal equipment, to the direction of travel, to the level of accuracy of the location information, to the identification of the network cell in which the terminal equipment is located at a certain point in time and to the time the location information was recorded'. **(d) Definition of 'communication' (para. 2(d)).** Within the framework of the Directive, the term 'communication' means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. Art. 5(1) states that traffic data are not included in the concept of communication where it imposes the confidentiality for 'communications and the related traffic data' (see comment on art. 5(1)). Recital 15 confirms this interpretation by indicating that 'a communication may include any naming, numbering or addressing information provided by the sender of a communication or the user of a connection to carry out the communication' while 'traffic data may include any translation of this information by the network over which the communication is transmitted for the purpose of carrying out the transmission'. Moreover, the communication does not include any information conveyed as part of a broadcasting service over an electronic communications network intended for a potentially unlimited audience, such as TV broadcasting. This exclusion marks the difference between the concept of 'communication' in the Directive and the concept of 'electronic communication' in the Framework Directive on electronic communications. Indeed, under the Framework Directive on electronic communications, the terms 'electronic communication network' and 'electronic communications services' include broadcasting services (see definitions under comment of para. 1, note 1(b)). Information conveyed as part of a broadcasting service will, however, still be considered a communication within the framework of the Directive when the information conveyed can be related to the identifiable subscriber or user receiving the information. This would for example be the case in the framework of the provision of video-on-demand services. The Directive thus only aims at including point-to-point communications which require an address to receive and send the communication, and exclude point-to-multipoint communications unless there is a possibility to identify the recipient of the communication. **(e) Definition of 'call' (para. 2(e)).** While extending the scope of application of the Directive to electronic communication, the Directive introduces a definition for the term 'call', proper to the telecommunication field. The Directive indeed still contains provisions specific to telephony services. A call means a connection established by means of a publicly available telephone service allowing two-way communication in real time. This includes mobile and fixed telephony. **(f) Definition of 'consent' (para. 2(f)).** The Directive indicates that the concept of consent of a user or a subscriber shall have the same meaning as in the definition provided for the terms 'data subject's consent' in the Data Protection Directive. According to art. 2(h) of the Data Protection Directive, these terms refer to 'any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed'. The consent must be free, specific and informed. This definition first of all implies that the consent is not obtained under any form of pressure. Economic or moral pressure could, for instance, possibly be an issue in a situation where the employee's consent is required in its capacity of user of a service involving the processing of its data and for which the employer subscribes. Moreover, the consent cannot be global; it must be granted for specific purposes of

processing of personal data. Finally, the consent must have been given on the basis of adequate information, that is, the information required by law. In some cases, such as in art. 5(3), the Directive specifically refers to the Data Protection Directive to identify the information to be provided. A particularity in this respect within the framework of the Directive is that the consent of legal person may be required by certain provisions of the Directive, whereas the Data Protection Directive only concerns individuals. The requirements with regard to the data subjects will therefore apply as such to subscribers regardless of the fact that they are legal persons. As to the manner according to which consent may be validly given, recital 17 of the Directive specifies that 'the consent may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes, including by ticking a box when visiting an internet website'. This mechanism envisaged by the Directive is already widely used on the internet and enables the internet user to express acceptance of a given option by selecting a box associated to this option. **(g) Definition of 'value added service' (para. 2(g)).** This is a new concept that did not exist in the Old Directive. It means any service which requires the processing of traffic data or location data other than traffic data beyond that which is necessary for the transmission of a communication or the billing thereof. The precision indicating that it concerns the processing of location data 'other than traffic data' is not absolutely necessary since location data not used for the purpose of conveying transmission of a communication will not be considered traffic data anyway (see definition of 'traffic data' under para. 2(b)). The range of services concerned is potentially very great since the only requirement is that in order to provide the service, the services provider needs to process either traffic data or location data but not in the context of the transmission of communication data. According to recital 30, 'any activity that goes beyond the transmission of a communication and the billing thereof and that is not based on aggregated data should be considered as value added service'. The value added services do not necessarily need to have a link with the related electronic communications service. Recital 18 gives several examples of value added services: advice on least expensive tariff packages, route guidance, traffic information, weather forecasts and tourist information. **(h) Definition of 'electronic mail' (para. 2(h)).** By this term, the Directive refers to any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient. This definition is intended to be technology neutral and to cover any message by electronic communications where the simultaneous participation of the sender and the recipient is not required. This concept is thus much broader than that of e-mail. It also includes SMS (Short Message Service), MMS (Multimedia Messaging Service), messages left on answering machines, voice mail service systems including mobile services and 'net send' communications addressed directly to an IP address (Opinion on unsolicited communications,

p. 4). Pop-up messages were however not considered by the European Commission as electronic mail (Answer to written question E-3392/02).

[Services concerned]

Article 3

(1) This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community.

(2) Articles 8, 10 and 11 shall apply to subscriber lines connected to digital exchanges and, where technically possible and if it does not require a disproportionate economic effort, to subscriber lines connected to analogue exchanges.

(3) Cases where it would be technically impossible or require a disproportionate economic effort to fulfil the requirements of Articles 8, 10 and 11 shall be notified to the Commission by the Member States.

1. Scope of the Directive (para. 1). *Services covered.* The scope of the Directive is defined as follows. It covers all the processing of personal data in connection with the provision of publicly available electronic communications networks in public communications networks. So unlike the old Directive, the scope is not confined to telephony or data networks but also encompasses satellite, terrestrial and cable TV broadcasting networks if of course the identification of the receiver is possible and that without consideration of the type of information conveyed. *Services excluded.* All the processing in connection with electronic communications networks which are not available to the public remain excluded, for example, services limited to closed-user groups or services not accessible through public communications networks, for example, through intranet even if these private networks are not limited to closed-user groups like automated teller machines offered in the context of banking services. This exclusion has been criticized by the Art. 29 Working Party underlining the fact that the distinction between public and private networks will be increasingly difficult to trace and taking into account the increasing importance of these private networks and the risks associated with their use, for example, the monitoring of the use of internet by employees within a company. Certainly if the services offered by companies to customers through their own private networks are excluded from the application of the Directive, they remain subject to the principles of the Data Protection Directive. Those principles require inter alia that the processing will be lawful, the data processed will be relevant and not excessive and the data subjects might exercise their rights to be informed, to access and to rectification.

2. Discussion (para. 2). *Lack of clarity.* The typical services covered by the Directive are not only those offered by the internet access provider, but also all services consisting in the conveyance of electronic signals at the specific request of the recipient of the service but not 'hosting services', content providers'

services or 'search engine services', which are indeed 'information society services' and are thereby excluded explicitly by the definition of electronic communication services given by article 2(c) of the Directive on a common framework for electronic communications networks and services: 'It (the concept of electronic communications services) does not include information society services as defined in article 1 of directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks.' Notwithstanding this clear exclusion, the wording used by the provision creates a certain ambiguity insofar as it refers to services 'in connection with the provision...' which could broaden, to a certain extent, the material scope of application of the Directive. The ambiguity increases when certain provisions of the Directive are considered that clearly have no meaning if they do not apply to these Information society services or other activities that do not consist 'strictly' of the 'conveyance' of electronic signals, like art. 13 on unsolicited e-mails or article 5(3) on illegal access to the terminal equipment of a subscriber or user. Nevertheless, most of the provisions only apply to providers or pure electronic communications services, like the provisions on traffic or location data, directories, automatic call forwarding, and so forth. One possible solution is to consider that the material scope of the Directive excludes the processing of personal data in the context of 'activities' that do not consist in providing publicly available electronic communications services on public communication networks, except when the text refers explicitly to other kind of 'activities' that cannot be identified with the concept mentioned in art. 3(1). Clearly articles like art. 5(3) on cookies or art. 13 on spam activities have a broader scope than that defined by art. 3(1).

3. Territorial scope of application (para. 3). The text refers to services provided 'in the Community'. Some of the services covered by the Directive might be offered to a subscriber or a user inside the European Union from a provider located outside the Community, for example, an internet access service. In that case, the text states clearly that the Directive is applicable. The criterion fixed by the Directive is not the same as the criterion of establishment retained by the General Directive and will thus permit to a certain extent an extraterritorial effect of this Directive. Notably, the spamming carried out by companies located outside of the Community will be subject to the EU provisions. As regards the services offered by companies operating within the Communities at the moment, it must be underlined that arts. 25 and 26 of the General Directive will apply in cases of cross-border data flows generated by a service offered by a provider located in the Community. It must be pointed out that it will frequently be the case with internet services insofar as the message is circulating through DNS and root servers located outside the EU. Art. 26(1)(b) of the Data Protection Directive, which provides an exception to the adequate protection when the cross-border data flow, is required for ensuring the performance of the contract between the provider and its customer.

4. Specific derogation for analogue exchanges (paras. 2 and 3). As regards communications services offered by analogue and non-digital exchanges, certain provisions of the Directive are not applicable if their application requires disproportionate efforts or if it is technically impossible. These provisions are listed: both arts. 8 and 10 on the presentation and restriction of calling and connected line identification and article 11 on automatic call forwarding. Under art. 3(3), the provider of these analogue exchanges must notify to the Commission that these conditions are met in order to benefit from this specific regime.

[Security]

Article 4

(1) The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.

(2) In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.

1. Obligation to take technical and organisational security measures (para. 1). *Principle.* This article imposes additional security obligations on the provider of a publicly available electronic communications service due to the specificity of the risks linked with the use of the networks. *Concept of 'security'.* The concept of 'security' is quite broad. It means under art. 17(1) of the Data Protection Directive protection 'against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other forms of unlawful processing'. So, for example, the risk of wiretapping by unauthorized third parties during the use of the services requires appropriate safeguards like the use of cryptography or secured lines (e.g. in case of electronic transmission of the credit card number). The possibility of intrusion within the provider's information system in order to collect all its customers' addresses or to manipulate certain data imposes the necessity to install firewalls and other security measures. The sending of worms through the information systems of a communications service provider or the creation of a mirror site in order to lead astray certain communication are other specific risks linked with the use of communications services. The obligation is not limited to technical measures but encompasses

also organizational measures which might be the nomination of a data security manager competent to ensure the compliance of the functioning of the service with all Directive provisions. In order to ensure such security, cooperation with the provider of the network might be desirable. Consequently, the operator of the network might be asked to intervene, if an intrusion is detected, to block automatically any access to the information system of the service provider. *Level of security.* The second sentence of para. 1 recalls the criteria developed by art. 17 of the Data Protection Directive to appreciate the level of security to be taken into account by the service provider. Thus, considering the potential risks linked with the nature of the service as regards both the probability of its occurrence and the harm that would result (an electronic communication service in the healthcare sector needs more security measures than a network permitting access to movies), attention will have to be paid both to the state of the art, that is, in particular the standards developed by such standardization institutes as ISO (on this point, reference might be made to the work of the ISO/IEC/ITU/UN ECE MoU Management Group and Privacy Technology Standards), and to the cost of the implementing the security measures. The more significant the risk, the higher the security level that must be achieved considering the cost of the implementing measures. As regards the kind of measures, emphasis should be placed on the importance of self-regulation in this realm: the development of standards; auditing methods; regimes for the approval of information systems, and so forth. The organizational and technical security of information systems must become an integral part of data protection policy. Finally, recital 20 of the Directive recalls the obligation of the electronic communications service provider to adapt continuously the level of security taking into account the evolution of the state of the art.

2. Duty to inform the subscribers (para 2). *Application.* In addition, the lack of network security and the proliferation of opportunities for illicit actions make it necessary for the providers of electronic communications services to be obligated to issue warnings concerning their use. Paragraph 2 answers this need. In case of 'particular' security risk, for example, the unexpected appearance of a worm, the discovery of certain failures in the security of its information system or the multiplication of attacks by hackers, the provider of the communications service has the duty to provide information about the existence of these risks and if no action against the risk is available for the service provider, it must alert the subscriber to the possible ways of avoiding the risk including the costs of these remedies, for example, it will advise using certain anti-spam or anti-spyware software. It is quite clear that this provision is applicable to internet access providers who will be requested in case of detection of certain illicit intrusions through their services to implement the appropriate security measures themselves in order to block these intrusions or subsidiary to give to their subscribers the adequate information about the way by which their customers might act against these threats. *Consequence.* The provision suggests that any breach of security will create a sort of 'prima facie' evidence that the service provider is liable if he is unable to demonstrate that he has given the information required or taken the appropriate measures (reversal of the burden of proof).

[Confidentiality of the communications]

Article 5

(1) Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.

(2) Paragraph 1 shall not affect any legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.

(3) Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user

1. General: the principle of confidentiality (para. 1). *Secrecy of correspondence.* The principle of the confidentiality of communications has been clearly asserted by theEuropean Court of Human Rights (see *Klass* (ECHR), *Malone* (ECHR), etc.) and derives directly from the art. 8 of the European Convention for the Protection of Human Rights (ECHR) which clearly asserts the secrecy of correspondence and must be interpreted as being applicable irrespective of the technical means used for conveyance (postal card, electronic mail or surfing, etc.). Thus, this principle forbids, as is the case for a postal card, any interference, any interception or surveillance of electronic correspondence. The wording used by the art. 5.1 does suggest a difference between 'communication' and 'traffic data'. *Communication* v *Traffic Data.* The concept of 'communication' is very wide, as mentioned above. It covers any information

exchanged, that is, the content of the message: the e-mail message sent or received; the web page visited; the movie or song sought by the user. This concept is clearly distinguished from the data identifying the communication (sender, receiver, protocol used, etc.) and necessary for conveying the message, that is, following the wording used by the European Directive: the traffic data which are also protected by the same principle according to the ECHR cases. The distinction will, however, permit more exceptions as regards the obligation of confidentiality for traffic data (see art. 6) than for communication (see infra, point 3).

2. Enforcement of the principle (para. 1). 'Members States shall ensure... through national legislation'. The Directive calls for at least legislative measures in the strict sense to establish the principle and its enforcement means. The adoption of a constitutional principle is not excluded and the legislation to be enacted must comply with the criteria adopted by art. 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms. The second sentence refers to a minimal intervention. 'The Member States shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data, by persons other than users, without the consent of the users concerned, except when legally authorised to do so, in accordance with Article 15(1)'. The text thus refers clearly to the recognition in each Member State of criminal offences related to these infringements in order to prevent third parties from intercepting electronic messages. Therefore, criminal legislation that punishes the classical wiretapping of voice telephony must be extended to all communication means. Other legislative measures might be contemplated, like provisions imposing professional secrecy on all persons in charge of conveying communications or the obligation for all or certain service providers subject to the obligation of confidentiality to be registered according to specific conditions ensuring respect of the condition, for example, nominating an internal audit service, adopting technical or organizational measures in order to prevent any infringements. In conclusion, the States' obligation to ensure confidentiality of communication might be viewed as a complementary duty to the service providers' obligation to implement the appropriate security measures under art. 4 of the Directive discussed above.

3. Exceptions (paras. 1 and 2). *Exception deriving from the scope of the Directive.* The principle as enunciated in the Directive does not cover the communications which are not conveyed by means of a public communications network and publicly available electronic communications services. Therefore, any communication by means of a private network or created in the context of a service not publicly available is not covered by the principle of confidentiality included in this piece of legislation but by the Council of Europe Human Rights Convention and certainly by the Data Protection principles of the Data Protection Directives as the lawfulness and proportionality of the processing, the rights of the subjects of the data and the security

principles. The Working Group has broadly criticized this restriction taking into account the same legitimate expectation of privacy existing in the two kind of networks. *Other exceptions explicitly mentioned by the Directive as regards 'communications'.* The Directive provides under art. 5(1) and (2) a certain number of exceptions to the confidentiality principle as regards communications. Other exceptions are laid down under art. 6 as regards traffic data. First exception: the users themselves might store the message they have received or sent. So it is quite obvious that a user might keep and use e-mail sent or received within the limit of respect of the Data Protection Directive principles as far as they constitute personal data. It must be underlined that this application will require that the collection be operated fairly, which implies, at least, that the subject concerned by these data might have reasonable knowledge of that processing. The second exception is based on the users' consent. Consent is not only required of the user receiving the message but also of the sender, which might be more difficult to obtain. As regards the form of the consent, one might refer to the requirements laid down by the art. 2 of the Data Protection Directive: 'any freely given specific and informed indication of his wishes by which the data subject signifies is agreement to personal data relating to him being processed'. The third exception relates to interceptions by security agencies or law enforcement authorities. It refers to art. 15(1), which will be discussed below. A fourth exception is provided for 'technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality'. Recital 22 comments extensively on this provision. These activities of 'automatic, intermediate and transient storage' will permit notably storing an e-mail until it is opened by the recipient or developing caching web pages, provided that any personal data related to the users having requested access to the web pages is erased. Para. 2 provides a fifth exception when the storage of a communication by a third party is part of a lawful business practice for the purpose of providing evidence of a commercial transaction. Three conditions are imposed to benefit from this exception: the storage must be legally authorized, according to recital 23, both parties to the communication must be informed of the recording and the data stored in this way must be 'erased as soon as possible and in any case at the latest by the end of the period during which the transaction can be lawfully challenged'. As regards concrete application of this exception, cases such as those of specific Healthcare or Banking networks conveying messages of great sensitivity for which traces must be kept might be quoted.

4. Intrusion into the terminal equipment of a subscriber or user (para. 3). *Principle.* Recital 24 does suggest an interesting comparison between the terminal equipment of a user and a private sphere similar to the domicile requiring protection under the European Convention for the Protection of Human Rights and fundamental freedoms. Any intrusion into the electronic domicile through spyware, web bugs, hidden identifiers, like cookies or other similar devices, ought to be considered a violation of the private electronic

space (virtual domicile), what could even be viewed as a form of hacking punished by criminal provisions. The provision clearly focuses on protection against intrusion mechanisms independent of the fact that personal data are processed or not through these mechanisms. *Legitimate use of certain devices.* These intrusions are strictly regulated even if recital 25 recognizes certain legitimate uses of some of these devices, for instance, cookies installed on a user's hard-disk in order to facilitate the provision of certain services or to verify the user's identity or capacity to conclude certain transactions. It is clearly stated that the use of these mechanisms might be justified on the grounds of legitimate purposes, for example, a session (not a permanent) cookie placed on the terminal equipment during the connection with a website offering travel services in order to be sure that if the connection is interrupted the user does not need to restate all the information already given. Recital 25 points out the fact that 'access to specific website content might be conditional on the well informed acceptance of a cookie or similar device, if it is used for a legitimate purpose'. Therefore, portals that offer access to multiple websites might invoke avoidance of charges as a reason for installing cookies as a condition for offering the services.

5. Conditions for their uses. Certain additional conditions are established by art. 5(3) for allowing the use of such devices. *Duty to inform.* Firstly, it is provided that users be informed clearly and precisely about the purposes of the data generated by the devices introduced into their terminal equipment in such a way to be sure that they are aware of the information being installed. This provision is a clear application of the right to be informed enacted by the Data Protection Directive as expressly asserted by recital 25. It implies that the name of the data controller and the purposes of the processing must also be given. This consequence is important insofar as many tracking devices are introduced by third parties (cyber marketing companies) in the context of invisible hyperlinks between them and the Information Society service called on by the internet user. It should be emphasized that by doing so the Directive recognizes that cookies are personal data, a point that has on occasion been contested in the past. The processing of data generated through these devices is subject to the other principles of the Data Protection Directive. For example, the duration of the placement of a cookie might be limited to the period justified by the legitimate purpose. This consideration is important insofar as, in many cases, cookies are placed for very long periods of time (20-30 years). *Opt-out system.* Second, users have no opt-in right as requested by privacy advocates but rather they have an opt-out right, in other words the right to refuse to have a tracking device placed on their terminal equipment. Recital 25 underlines the obligation to offer this right to refuse through user-friendly methods. Finally, according to the same recital, 'the information and right to refuse may be offered once for the use of devices during the same connection and also covering any further use that may be made of those devices during subsequent connections'.

6. Exceptions to the opt-out system. Two exceptions to the opt-out system are provided by the Directive. The first one mentions the necessity of 'storage and access for the sole purpose of carrying out or facilitating the transmission of a communication'. Authors believe this exception could allow, for example, a software feature that searches users' address books to obtain e-mail addresses without requesting these from the users themselves. The addresses would then be used for the purpose of sending (unsolicited) e-mails. The second exception expressly mentioned by the last sentence of para. 3 refers to any technical storage or access 'strictly necessary in order to provide an information society service explicitly requested by the subscriber or user'. The text refers to tracking devices which are strictly necessary and not simply useful, for instance, screen simulator software which renders downloading certain web pages more user-friendly. Furthermore, is it possible to consider that a software seller needs to install 'spyware' within the user's terminal in order to verify whether there is no contra-indication as regards the functioning of the software to be purchased? Under such circumstances, the opt-out solution, consisting in alerting the user to the installation of the device and the reasons why it is desirable, seems more appropriate.

[Traffic data]

Article 6

(1) Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).

(2) Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.

(3) For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his/her consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.

(4) The service provider must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing for the purposes mentioned in paragraph 2 and, prior to obtaining consent, for the purposes mentioned in paragraph 3.

(5) Processing of traffic data, in accordance with paragraphs 1, 2, 3 and 4, must be restricted to persons acting under the authority of providers of the public

communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.

(6) Paragraphs 1, 2, 3 and 5 shall apply without prejudice to the possibility for competent bodies to be informed of traffic data in conformity with applicable legislation with a view to settling disputes, in particular interconnection or billing disputes.

1. General. This provision governs the processing of traffic data in the context of the provision of a public communications network and of publicly available electronic communications services. It specifies the purposes for which traffic data may be processed, the conditions for such processing and the persons who may legally process the data. Since traffic data are, in principle, confidential by virtue of art. 5 (see comment on art. 5(1)), the present provision allowing the processing of such data for specific purposes should be viewed as derogating from this principle and should be interpreted restrictively. Moreover, the requirements set for traffic data processing in this article are not the only ones applicable. Indeed, the Data Protection Directive applies to all the aspects that are not specifically regulated in the present art. 6. For instance, if traffic data are personal data, the data controller is required to comply with the general requirements stated in the Data Protection Directive such as the obligation to notify the processing to the supervisory authority (art. 18 of the Data Protection Directive) or the condition only to process data that are adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed (art. 6 of the Data Protection Directive). Recital 30 of the Directive expressly indicates in this regard that 'systems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum'.

2. Retention of traffic data (para. 1). (a) The erasure rule. Para. 1 states that the provider of a public communications network and the provider of publicly available electronic communications services cannot process or store traffic data longer than necessary for the purpose of the transmission of the communication processed. Para. 1 clearly authorizes the processing of traffic data by these providers for a transmission purpose while it sets limits to such processing. Furthermore, recital 29 of the Directive allows the processing, in individual cases, of traffic data by the service provider where this is necessary in order to detect technical failure or errors in the transmission of communications. The provider of public communications network and the provider of publicly available electronic communications services must erase traffic data or render them anonymous as soon as the retention of the traffic data is no longer necessary to ensure the transmission of a communication.

Recital 27 concedes that the exact moment of the completion of the transmission of a communication depends on the type of electronic communications service that is provided. A telephone call will be ended as soon as either of the users terminates the connection while the transmission of an electronic mail is completed as soon as the addressee collects the message, typically from the server of the service provider. According to recital 28, 'the obligation to erase traffic data or to make such data anonymous when it is no longer needed for the purpose of the transmission of a communication does not conflict, however, with such procedures on internet as the caching in the domain name system of IP addresses or the caching of IP addresses to physical address bindings or the use of log-in information to control the right of access to networks or services'. The exact intention of the European legislator when inserting such recital is unclear. It is likely that such commentary aims at allowing retention of traffic data for the purpose of caching or log-in procedures in spite of the erasure rule. **(b) Rule applies to traffic data relating to users and subscribers.** This erasure rule applies to traffic data relating to subscribers as well as to traffic data concerning users. Therefore, the processing of data relating to legal persons who are subscribers is subject to the limitations stated in this paragraph. **(c) Exceptions.** Retention and further processing of traffic data after transmission is completed is however admitted for specific purposes identified in para. 2, 3 and 5 and in art. 15(1).

3. Traffic data processing for billing purposes (para. 2). (a) Purposes of processing allowed. Traffic data relating to users and subscribers may be processed for billing purposes and interconnection payment. Processing for billing purposes seems perfectly logical since traffic data are precisely identified as data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof (see commentary on art. 2(2)(b)). **(b) Selection of the traffic data.** Only the traffic data in the possession of the service provider which are necessary to carry out the billing and payment procedures may be stored and further processed longer than permitted under para. 1. The traffic data processed will thus need to be selected with regards to the type of billing carried out. For instance, non-itemized billing will not require as much data as itemized billing. **(c) Duration of the retention.** Moreover, traffic data can only be retained for the period during which the bill may lawfully be challenged or payment pursued. This period may vary between Member States as no precise time limit is defined in the Directive. The Working Party issued a recommendation to Member States in this regard. The Working Party considers that this should ordinarily involve a routine storage period for billing of maximum 3-6 months, with the exception of particular cases of dispute where the data may be processed for a longer period (Opinion on storage of traffic data for billing purposes, pp. 6-7). **(d) Information requirement (para. 4).** *Content of the information.* Para. 4 goes beyond

the regime of the Old Directive in requiring from the service provider to supply specific information to the subscriber or user in respect of the use of their data for billing purposes and interconnection payment. The service provider must indeed inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing, as well as of the purposes of processing, i.e. the purposes of billing and/or interconnection payment. *Moment of the information.* Although para. 4 does not indicate when the information needs to be provided, it is reasonable to consider that the information should be supplied prior to carrying out the related processing. This position is also supported by the fact that prior information is the rule under art. 9 of the Data Protection Directive. In line with this, the explanatory memorandum of the Proposal for the Directive explains that 'the information obligation aims at empowering the subscribers to control and, where necessary, to object to ongoing data processing'. Recital 26 goes even further and states that service providers should always keep subscribers informed of the types of data they are processing and the purposes and duration for which this is done. This implies that service providers should not only provide initial information but also update the information when there is a change in the data processed or the duration of processing. *Subject of the information.* Para. 4 indicates that the service providers may inform either the subscriber or the user. In many cases it will however be impossible to inform the user when he/she is not known to the service provider. In some cases, such as in respect of internet access services, there might also be several users for a same service.

4. Traffic data processing for the purpose of marketing electronic communications services and for the provision of value added services (para. 3). (a) Purposes of processing allowed. Para. 3 allows the provider of a publicly available electronic communications service to retain and further process traffic data relating to subscribers and users for the purpose of marketing electronic communications services or of providing value added services. The marketing of electronic communications services may potentially concern services provided by the provider of a publicly available electronic communications service as well as services provided by third parties. Indeed, where the text of the Old Directive envisaged the processing of traffic data by the provider of a publicly available electronic communications service for the marketing of its own electronic communications services, the wording of the Directive uses the neutral terminology of 'marketing electronic communications services'. The Directive also extends the possibility of processing traffic data to the provision of 'value added services'. A definition of value added services is provided in commentary on art. 2(2)(g)). **(b) Selection of the traffic data.** Only the traffic data which are necessary for such services or marketing can be stored and processed for the period necessary to carry out these activities. The data should be erased or made anonymous after the provision of the service. **(c) Consent.** *Requirement of the consent of the user or of the subscriber.* Traffic data can only be processed for the purpose of marketing electronic communications services or of providing value added services provided that the subscriber or user to whom the data relate has given his/her consent. This would imply that in any case the service provider would need to identify whose data are processed (the subscriber's or the user's) and manage to obtain the consent of the data subject. Recital 31 seems however to be more nuanced when it states that 'whether the consent to be obtained for the processing of personal data with a view to providing a particular value added service should be that of the user or of the subscriber, will not only depend on the data to be processed and on the type of service to be provided but also on whether it is technically, procedurally and contractually possible to distinguish the individual using an electronic communications service from the legal or natural person having subscribed to it'. If we consider the example of an internet access provider offering customized services including value added services, it will be likely more appropriate to ask the consent from the subscriber at the moment of the subscription for the service if the content of the service cannot actually be adapted afterwards in consideration of the person using it (the subscriber or the user). On the other hand, when value added services can be customized by the user itself (for instance, by the GPS user or the voice telephony services users), there is no reason for not seeking to obtain his/her consent. *Definition of 'consent'.* As, mentioned in our comment of art. 2(2)(f), the consent of a user or subscriber referred to in the Directive has the same meaning as the data subject's consent as defined and further specified in the Data Protection Directive, regardless of whether the latter is a natural or a legal person. According to recital 17, consent may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes, including by ticking a box when visiting an internet website. *Right of withdrawal.* Moreover, users or subscribers must be given the possibility to withdraw their consent for the processing of traffic data at any time. This does not only mean that the user or subscriber has the right to withdraw his/her consent at any time but it also requires that he/she is given the effective possibility to do so. The withdrawal prevents the service provider from processing the data subject's data in the future. **(d) Information.** *Content of information.* In addition, the service provider must, in respect of para. 4, inform the subscriber or user of the types of traffic data which are processed, and of the duration and purposes of such processing. *Moment of information.* The information must be provided prior to obtaining the consent. *Subject of information.* With regard to the informed consent requirement, the duty of information appears to entail that at least the person who has to consent to the use of its data either for marketing purposes or for the provision of value added services will need to receive the information.

5. Other purposes of processing (para. 5). Para. 5 implicitly admits purposes of processing that are not envisaged under para. 1, 2 and 4. It indeed considers that persons handling customer enquiries or fraud detection are entitled to

process traffic data. This explicit reference to activities not mentioned in the above paragraphs of art. 6 suggests that processing of these purposes is allowed. It is remarkable that while evoking these purposes, the Directive does not provide for any specific conditions with respect to the connected processing. The processing of these data will however be subject to the conditions set in the Data Protection Directive as far as they are personal data. With respect to fraud detection, it is moreover likely that only internal fraud with regard to the electronic communications services is concerned and not criminal investigation, which is reserved to public authorities (see comment on art. 15). Recital 29 appears to be even more restrictive and only to consider the processing of certain traffic data for fraud detection as it indicates that 'traffic data necessary for billing purposes may also be processed by the provider in order to detect and stop fraud consisting of unpaid use of the electronic communications service'.

6. Persons entitled to process traffic data in framework of para. 1, 2, 3 and 4 (para. 5). (a) The service provider's personnel. Para. 5 identifies the categories of personnel of the service provider who may carry out the processing. It further specifies that the processing must be restricted to what is necessary for the purposes of the sectors of activities mentioned. The processing of traffic data must be restricted to persons acting under the authority of the service provider and who need to process the data in the framework of their function, namely, handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or the provision a value added service. As stated above, the right to process traffic data for the purpose of marketing electronic communications services or of providing value added services is only granted to the provider of publicly available electronic communications services and not to providers of the public communications networks. Therefore only the personnel acting under the authority of the providers of publicly available electronic communications services is entitled to process traffic data for this purpose. **(b) Communication to third parties.** Para. 5 does not envisage a possible communication of traffic data by the service provider to a third party. Recital 32 seems however to allow the communication of traffic data to a third party providing value added services when it states that 'where the provision of a value added service requires that traffic or location data are forwarded from an electronic communications service provider to a provider of value added services, the subscribers or users to whom the data are related should also be fully informed of this forwarding before giving their consent for the processing of the data'. Para. 5 could be construed as allowing such communication provided that the value added service provider remains under the authority of the electronic communications service provider. Such interpretation would however create a level of protec-tion for traffic data which is stronger than the one granted under art. 9 to location data, being more sensitive than traffic data. Indeed, communication of location data to a value added services provider is expressly allowed (see commentary on art. 9). It is therefore reasonable to consider that traffic data may be forwarded to a provider of value added service without requiring that the latter remains under the authority of the service provider. In case of such a forwarding of data, the user or subscriber would need to receive specific information about the processing of the data without prejudice to the application of all other rules arising from the Data Protection Directive as to a communication of personal data (especially art. 6(b) of the Data Protection Directive). **(c) Subcontracting of services.** Para. 5 considers the processing of traffic data by persons acting under the authority of the service provider but does not envisage as such the subcontracting of part of or of the whole processing carried out by the service provider on traffic data to a processor (in the sense of art. 17 of the Data Protection Directive). Indeed the terms 'under the authority of' do not refer to the characteristics of a subcontracting of data processing to a processor. Art. 17(3) of the Data Protection Directive indeed does not strictly require the processor to act under the authority of the data controller but only specifies that the parties agree in a contract that the processor shall only act on instructions of the data controller. However, recital 32 explicitly regulates that 'where the provider of an electronic communications service or of a value added service subcontracts the processing of personal data necessary for the provision of these services to another entity, such subcontracting and subsequent data processing should be in full compliance with the requirements regarding controllers and processors of personal data as set out in the [Data Protection Directive]'. Therefore, the communication of traffic data in the framework of a processing agreement for the provision of value added services is not excluded. For instance, an internet service provider could subcontract a value added service consisting in an assistance to navigate on internet to a processor and, in this framework, could transfer the internet addresses requested by its subscriber. In such a case, the service provider is also required to inform the users and subscribers about the forwarding of their data before they give their consent where such consent is required (i.e., in case of provision of value added services).

7. Communication of traffic data to competent bodies (para. 6). According to para. 6, para. 1, 2, 3 and 5 apply without prejudice to the possibility for competent bodies to be informed of traffic data in conformity with applicable legislation with a view to settling disputes, in particular interconnection or billing disputes. This paragraph introduces an additional purpose, the settlement of disputes, of processing allowing the service provider to disclose traffic data to competent bodies and the competent bodies to process traffic data where such processing is in conformity with the applicable legislation. The consequences of the use of the terms 'without prejudice' are not very clear: would this paragraph allow the storage of data longer as permitted under paragraphs 1, 2, 3 and 5 in view of a possible communication to a competent body?

[Itemised billing]

Article 7

(1) Subscribers shall have the right to receive non-itemised bills.

(2) Member States shall apply national provisions in order to reconcile the rights of subscribers receiving itemised bills with the right to privacy of calling users and called subscribers, for example by ensuring that sufficient alternative privacy enhancing methods of communications or payments are available to such users and subscribers.

General. Para. 1 gives the subscriber the right to obtain itemized bills for all services covered by the Directive and not only for voice telephony services as it was the case with the Old Directive or the Universal Service Directive (Booklet 1-4). The significance of this provision is unclear as it might mean that the offer of an itemized billing is only optional and submitted to the condition of the subscriber's request. Para. 2 encourages the Member States to take national measures in order to 'reconcile the rights of subscribers receiving itemized bills with the right to privacy of calling users and called subscribers'. *Consumers' v Privacy concerns - Possible solutions.* On that point precisely, consumer protection interests might diverge substantially from privacy concerns. The problem is delicate insofar the subscriber might be different from the user, for example, within a family or a company. In that context the itemized bill might be a way to have a look at the activities of an employee or a spouse or child. To solve this delicate problem, recital 33 does suggest certain methods like the use of optional services and payment mechanisms (e.g. prepaid calling cards to be inserted in the terminal equipment) which will permit use of the terminal equipment anonymously and without traces in the bill. Furthermore, at the request of the Working Party, the same recital makes reference to the French solution enacted by Decree No. 2002-36 of 8 January 2002 which requires voice telephony service providers to offer a service option whereby the last four digits of the called numbers do not appear on the bill.

[Presentation and restriction of the calling and connected line identification]

Article 8

(1) Where presentation of calling line identification is offered, the service provider must offer the calling user the possibility, using a simple means and free of charge, of preventing the presentation of the calling line identification on a per-call basis. The calling subscriber must have this possibility on a per-line basis.

(2) Where presentation of calling line identification is offered, the service provider must offer the called subscriber the possibility, using a simple means and free of charge for reasonable use of this function, of preventing the presentation of the calling line identification of incoming calls.

(3) Where presentation of calling line identification is offered and where the calling line identification is presented prior to the call being established, the service provider must offer the called subscriber the possibility, using a simple means, of rejecting incoming calls where the presentation of the calling line identification has been prevented by the calling user or subscriber.

(4) Where presentation of connected line identification is offered, the service provider must offer the called subscriber the possibility, using a simple means and free of charge, of preventing the presentation of the connected line identification of the calling user.

(5) Paragraph 1 shall also apply with regard to calls to third countries originating in the Community. Paragraphs 2, 3 and 4 shall also apply to incoming calls originating in third countries.

(6) Member States shall ensure that where presentation of calling and/or connected line identification is offered, the providers of publicly available electronic communications services inform the public thereof and of the possibilities set out in Paragraphs 1, 2, 3 and 4.

1. General. This article, which remained basically unchanged when the Old Directive was replaced in 2002, regulates in detail the conditions under which information about the participants in a telephone conversation may be disclosed and presented to the other party before this conversation starts or during the conversation. The need for such regulations arose with the roll-out of digital telephone networks and the use of telephone terminals with displays. In analogue networks there was neither a need nor a technical possibility to transmit information about the calling subscriber or calling user (the term 'callers' is used in the following text when it applies to both groups of callers) to the called subscriber or called user (the term 'callees' is used in the following text when it applies to both groups of callees). Callers remained anonymous before they identified themselves after the connection had been established. With the advent of digital telecommunications networks the data about calling and called subscribers had to be exchanged in order to establish a connection between them. The number of the calling subscriber is sent via the networks (several networks, i.e., several carriers may be involved if the called subscriber has a contract with a different carrier from the calling subscriber). This transmitted information is not only disclosed to the network carriers but also to the participants in the communications as long as their terminal equipment is fitted with displays or linked to a computer. Even in analogue networks digital terminals may be used, which has been the case in several Member States in the transitional period before complete digitalization of networks. When Voice over IP is used and computers with speakers function as terminals, the same applies since the calling or called numbers may be presented on the screen. This is of particular economic interest to companies taking orders via telephone, to other distance-selling businesses or to call centres. In digital networks they can identify incoming calls before taking the

call and prepare for the conversation by searching their databases depending on whether the caller is an existing or a new customer and if the caller is an existing customer, what the status of any transactions with them may be. Thus calling line identification may on the one hand improve the service for the customer whose request may be dealt with more efficiently. Nevertheless, both participants in the communications (callers as well as callees) may have a legitimate interest to control the disclosure as well as further use of the data which may be transmitted and disclosed before and during the conversation over the phone in addition to the content data. Callers might be interested in staying anonymous when calling a help-line or in identifying themselves in order to receive some initial information from a company but may not want their data stored in a database at the callee's end at this stage or in general. The Data Protection Directive limits the processing of such data apart from the electronic communications and after it has finished but this article provides for the necessary additional protection of the caller's privacy before any controller may receive the callee's data and process them without the knowledge of the data subject. The callee may, however, have a legitimate interest to communicate only with callers who are willing to identify themselves. The technology allows for negotiating the conditions of exchange of personal data before the communications even start. The article provides for the privacy-friendly use of digital networks by spelling out obligations for service providers with regard to the functionality of presentation of calling line identification. There is no obligation to present calling line identification in the first place, but makes specific provisions if this function is offered. Art. 8 refers with its language ('calling line') to voice telephony where the privacy debate on this issue started, that is, in the US. But the provision applies to other electronic services as well (the Working Party differed on this when stating that the provision applied only to conventional voice telephony, not Voice over IP, IP addresses and e-mail, see Working Paper 36). With regard to e-mail, art, 13(4) makes special provision for unsolicited communications which takes precedence over art. 8 (see the commentary on art. 13(4)). When sending electronic mail for the purpose of direct marketing the sender may not disguise or conceal its identity; the sender cannot rely on art. 8. However, when surfing the World Wide Web users are allowed to do so anonymously by using anonymizers or equivalent services in order not to disclose their identity. The privacy options to prevent the presentation of calling line identification offered on a per-line basis do not have to be available as an automatic network service; they can also be obtained through a simple request to the provider of the publicly available electronic communications service (other than the network carrier, see recital 34). Providers may not be exempted from the obligations in accordance with art. 8 on the grounds of costs. However, the application of these obligations should not be made mandatory in specific cases where subscriber lines are connected to analogue exchanges and the application would either be technically impossible or would require a disproportionate economic effort. Interested parties as well as the Commission should be informed of such cases

(see recital 19). When the Old Directive was drafted initially by the European Commission, it did not contain provisions which are now laid down in art. 8. It is to a large extent due to the proposals made by Data Protection Commissioners in the Member States and on the European level that the article was phrased in its present form. Art. 8 does not regulate whether and to what extent personal information including or based on calling line identification may be processed by the recipient (e.g., a call centre or a distant selling company). This is covered by the Data Protection Directive.

2. Option to prevent calling line identification of outgoing calls (para. 1). Whereas the Old Directive only stated that callers should have the possibility to eliminate the presentation of calling line identification, art. 8(1) of the Directive specifically obliges the Member States to create a duty for the service providers to offer this possibility. Callers have to be able to eliminate calling line identification via a simple means and free of charge. This does not apply to the transmission of information identifying the calling line since this is a technical prerequisite for establishing the connection in digital telecommunications networks. The right to block this information refers to its presentation on the callee's terminal. The term 'simple means' is rather unclear. This important technical requirement may be met by the service provider by offering a network-based function which blocks calling line identification from being sent from the last exchange or router to the callee if this is possible without preventing the connection being established. It is more likely to be met by a function which sends an additional signal with the calling line identification that it must not be shown on the callee's terminal (provided that this terminal has the technical features for showing, i.e., a display). In both cases the caller's terminal hardware must support these functionalities either with a 'blocking button' or by dialling a certain combination of digits. The Directive furthermore distinguishes between calling users and calling subscribers: Whereas users must have the blocking facility on a per-call basis the subscribers must have this possibility on a per-line basis. The reason for this distinction seems to be that the user who uses the terminal equipment of another person (the subscriber) cannot influence the terms of the contract between this subscriber and the service provider. In addition, the user will have no interest to do so but will simply want to suppress the calling line identification with regard to that particular call (on a case-by-case basis). The subscriber, however, may have a legitimate interest to block calling line identification permanently on a per-line basis. But art. 8(1) does not take into account that a subscriber may equally have a legitimate interest in blocking calling line identification on a case-by-case basis. This may not be a practical problem if the terminal equipment allows for simple blocking of calling line identification either on a per-call basis or on a per-line basis.

3. Option to prevent calling line identification of incoming calls (para. 2). Similarly the callee may have a legitimate interest that calling identification of incoming calls is not shown on their terminal. Other persons (e.g., family

members) may be present when the call comes in and the called person may not want to disclose the caller's identity. Fixed and mobile terminals would force them to accept this disclosure to third persons if the appearance of the caller's number on the display cannot be suppressed. Also help lines, counselling services (e.g., for HIV issues) and similar organisations have a vital interest to guarantee the anonymity of their callers regardless of the terminals they are calling from (see recital 34). They want to establish a trust relationship over the phone or the internet and encourage people to contact them through these channels; to this end they have to make sure that calling line identification is not shown them even if the caller has for whatever reasons not taken measures to prevent this. As stated, this is not only a question of terminal hardware but also of a requirement laid down by the Directive for service providers to offer and support this blocking function in the network. The duty is limited to subscribers. Again it could be argued that called users (who are not subscribers for the terminal where the call arrives) should have the option, too, of suppressing the identification of incoming calls. Privacy-enhancing terminal hardware should solve this problem. Para. 2 differs from para. 1 in one respect: it only obligates offering this blocking function free of charge 'for reasonable use of this function' (whereas para. 1 does not contain this restriction). It is not clear what kind of possible unreasonable use the authors of the Directive had in mind. Service providers cannot rely on this provision when trying to limit the use of the blocking function quantitatively.

4. 'Block-blocking option' (para. 3). The interest of callers to withhold their identification in communications networks cannot be seen as isolated or unrestricted. Their counterpart, the called person, may also have a legitimate interest in identifying the calling person. They may decide to restrict their communications to partners who are prepared to identify themselves. Since modern technology supports a process of negotiations about the conditions of communications the Directive contains an obligation for service providers to offer such a negotiation function before the connection is established. The called subscriber can opt to reject all incoming calls where the caller has prevented the calling line identification from being displayed. In this case the callers should receive a signal informing them of the rejection; they may then decide to change the initial decision not to disclose the calling line identification if they choose to do so. This again shows that the calling subscriber (not only the calling user) should have the option of deciding whether to prevent calling line identification on a per-call basis to allow for a flexible negotiation process (see para. 1 above which only prescribes this option for calling subscribers on a per-line basis).

5. Option to prevent connected line identification of incoming calls (para. 4). In the case of connected networks the called party has the right to prevent the presentation of the identification of the line to which the caller is actually connected. Recital 34 refers to the case of forwarded calls but this seems not to be the most relevant example. Nowadays in a competitive environment most

communications networks are connected and it would make little sense if the option to prevent the line identification of incoming calls would be restricted to 'unconnected' lines. The additional practical effect of this provision in relation to para. 2 is therefore doubtful.

6. Transborder calls (para. 5). The Directive extends its legal protection with regard to privacy options in the case of calling line identification to cross-border calls to third countries originating in the Community as well as incoming calls received in the Community originating in third countries. This is in line with the Data Protection Directive which provides for a mechanism to ensure that personal data will only be transferred to third countries if there is an adequate level of protection or equivalent safeguards in these countries. The XIIth International Conference of Data Protection Commissioners (1990) stressed the need for applying data protection standards and options to international calls. However, art. 8(5) of the Directive is much less explicit as to how the provisions of paras. 1-4 may be implemented with regard to cross-border calls. The authors of the Directive have not taken up a suggestion made in a Memorandum from the International Working Group to provide for the automatic suppression of calling line identification information in cases where the caller has asked for the elimination of this information when making a call to a State where the provisions of para. 1 have not been implemented. In the absence of such a provision Member States have to oblige service providers in the Community to integrate these privacy options when negotiating roaming or interconnection agreements with providers in third countries.

7. Duty to inform the public (para. 6). Data subjects can only make an informed choice about privacy facilities they may want to use if they have been informed of the existing options. Therefore Member States have to ensure that the providers of publicly available electronic communications services inform the public whether they are offering calling and/or connected line identification and about the privacy options provided for in paras. 1-5 (see recital 34). Interested parties should also be informed of cases where it is technically impossible or would require a disproportionate economic effort to comply with the requirements of paras. 1-5 in cases of subscriber lines connected to analogue exchanges (see recital 19).

[Location data other than traffic data]

Article 9

(1) Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added

service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time.

(2) Where consent of the users or subscribers has been obtained for the processing of location data other than traffic data, the user or subscriber must continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.

(3) Processing of location data other than traffic data in accordance with paragraphs 1 and 2 must be restricted to persons acting under the authority of the provider of the public communications network or publicly available communications service or of the third party providing the value added service, and must be restricted to what is necessary for the purposes of providing the value added service.

1. General. This provision governs the processing of certain location data obtained in the context of the provision of a public communications network and of publicly available electronic communications services. Indeed it exclusively governs the processing of certain location data, that is, those that are not to be considered traffic data. The processing of location data which are a by-product of the communication transmission service remain, as before under the Old Directive, governed by art. 6 of the Directive. The European Commission noticed that, since the adoption of the Old Directive, technologies involving the processing of data allowing the exact positioning of a mobile user's terminal equipment (such as the Global Positioning System (GPS)) had been emerging. These technologies support the provision of new services, such as road transport telematic services providing traffic information and guidance to drivers, and allow the exact positioning of a mobile user's terminal equipment. Therefore, the European Commission considered it necessary to define a specific regime for the processing of these data ensuring appropriate data protection and privacy safeguards. The requirements imposed in art. 9 are not the only ones applicable to the processing of location data. As explained in the commentary on art. 6, the Data Protection Directive remains applicable for all the aspects that are not specifically regulated by the Directive (see comments in this regard under art. 6, note 1).

2. Processing of location data other than traffic data (para. 1). (a) Prohibition of processing and exception. Para 1. states that where processing of location data other than traffic data is possible, it can only be carried out on anonymous data or for the purpose of providing value added services. **(b) Provision of value added services.** *Requirement of the consent of the user or of the subscriber.* The processing of location data carried out in the framework of the provision of a value added service is however subject to the prior consent of the subscriber or of the user. As mentioned in the commentary on art. 6(3), recital 31 states that whether the consent to be obtained for the processing of personal data with a view to providing a particular value added service should be that of the user or of the subscriber will not only depend on the data to be processed and on the type of service to be provided but also on whether it is technically, procedurally and contractually possible to distinguish the individual using an electronic communications service from the legal or natural person having subscribed to it. *Definition of 'consent'.* The requirements regarding the consent to be provided by the subscriber or the user are the same as those specified in the Data Protection Directive, also for what concerns a legal person's consent. According to recital 17, the consent may be given by any appropriate method such as ticking a box when visiting an internet website as long as the consent is a freely given, specific and informed indication of the user's wishes. Special regulations have been created regarding the processing of location data by organizations dealing with emergency calls in spite of the absence of consent for the processing of such data (see commentary on art. 10(b)). *Right of withdrawal.* Moreover, users or subscribers must be given the possibility to withdraw, at any time, their consent for the processing of location data. This not only requires that the user or subscriber have the right to withdraw its consent at any time but also that they are given the effective possibility to do so. The withdrawal prevents the service provider from processing the subject's data in the future. *Right of temporary refusal of the processing.* Para. 2 provides that the user or subscriber must be offered, in addition to the right of withdrawal, the possibility to refuse temporarily the processing of location data other than traffic data for each connection to the network or for each transmission of a communication. Regarding the modalities of this refusal process, the Directive only specifies that such temporary refusal must be free of charge and should be rendered possible by the use of a simple means. The Directive does not, however, indicate whether the refusal can be contemplated as a refusal per connection or transmission or it should be conceived as a refusal over a certain period. The temporary refusal of a subscriber or user for the processing of location data does not, however, impede the processing of such data for organizations dealing with emergency calls under certain conditions (see commentary on article 10(b)). **(d) Information.** *Content of information.* In addition, the service provider must, in respect of para. 4, inform the subscriber or user of the types of traffic data which are processed, and of the duration and purposes of such processing. *Moment of information.* The information must be provided prior to obtaining the consent. *Subject of information.* As the information should be provided prior to the consent given by the user or the subscriber for the use of its data either for marketing purposes or for the provision of value added services, at least the person who will have to consent would need to receive the information.

3. Persons entitled to process location data in the framework of para. 1 and 2 (para. 3). (a) Persons acting under the authority of the service provider. Para. 3 specifies that the actual processing of location data other than traffic data carried out in accordance with paras. 1 and 2 should be restricted to the personnel who is acting under the authority of the provider of the public communications network or publicly available communications service or of the third party providing the value added service. Moreover, the processing must be limited to what is strictly necessary to provide the value added services. This excludes that the provider of a value added service carries out processing on the location data other than traffic data in view of promoting its services, as allowed in the framework of the processing of traffic data (see comment on art. 6(3)). **(b) Communication to third parties.** Para. 3 does implicitly envisage a possible communication of location data other than traffic data by the service provider. Indeed, the provider of value added services is mentioned as one of the specific categories of service providers under the authority of which location data other than traffic data can be processed. This involves a communication of location data other than traffic data from the provider of the public communications network or from the provider of publicly available communications service who originally are the only ones retaining such location data. Moreover, as mentioned in the commentary on art. 6(3), recital 32 expressly envisages the communication of location data to a third party providing value added services as it sets a condition to the forwarding of data by an electronic communications service provider to a provider of value added services and requires that the subscribers or users to whom the data are related are fully informed of this forwarding before giving their consent for the processing of the data. **(c) Subcontracting of services.** Para. 3 only concerns the processing of location data other than traffic data by persons acting under the authority of the service provider but does not consider subcontracting part of or the whole processing carried out by the service provider on traffic data to a processor (in the sense of art. 17 of the Data Protection Directive). As mentioned in the commentary on art. 6, the reference to the terms 'acting under the authority' of a controller does not amount to an authorization to subcontract the processing to a processor. Nevertheless, recital 32 seems to allow such subcontracting as it states that 'where the provider of an electronic communications service or of a value added service subcontracts the processing of personal data necessary for the provision of these services to another entity, such subcontracting and subsequent data processing should be in full compliance with the requirements regarding controllers and processors of personal data as set out in the [Data Protection Directive]'. Therefore, the subcontracting of the processing of location data by an electronic service provider or by a value added service provider is not excluded. For instance, a provider of telephony services could provide location data to a third company in the framework of a processing agreement to provide end customers with weather forecast information or tourist information based

on their location data. In such a case, the service provider is required to inform the users and subscribers about the forwarding of their data before they give their consent to the processing of location data other than traffic data for the provision of value added services.

[Exceptions]

Article 10

Member States shall ensure that here are transparent procedures governing the way in which a provider of a public communications network and/or a publicly available electronic communications service may override:

(a) the elimination of the presentation of calling line identification, on a temporary basis, upon application of a subscriber requesting the tracing of malicious or nuisance calls. In this case, in accordance with national law, the data containing the identification of the calling subscriber will be stored and be made available by the provider of a public communications network and/or a publicly available electronic communications service;

(b) the elimination of the presentation of calling line identification and the temporary denial or absence of consent of a subscriber or user for the processing of location data, on a per-line basis for organisations dealing with emergency calls and recognised as such by a Member State, including law enforcement agencies, ambulance services and fire brigades, for the purpose of responding to such calls.

1. Aim of the provision. Art. 10 provides for exceptional cases where the caller's privacy choice to prevent the display of calling line identification under art. 8 (1) may be overridden either in the interest of the called subscriber or in the interest of the public in general. Subscribers or users can then be identified or located against their will. The Directive does not require Member States to provide for such an override but if they do so they have to establish transparent procedures which providers must follow before overriding the caller's choice to prevent calling line information from being displayed.

2. Tracing malicious calls (para. a). The callee has a legitimate interest to be protected against malicious or nuisance calls. An override of the elimination of caller identification may therefore be applied for on a temporary basis in order to trace malicious or nuisance calls (i.e., identify the caller). If an override takes place the network or service provider is allowed within the limits of national law to store the data identifying the calling subscriber. The Article does not mention a time limit for this storage but it is obvious that the data have to be erased once they are no longer necessary in this particular case. Furthermore they may not be used by the provider for any purpose other than tracing the calls in question. The Directive allows for the 'making available' by the provider without any restriction. It seems adequate that they are disclosed to

the subscriber applying for the override who may then institute proceedings (civil or criminal) against the identified malicious caller.

3. Override in the public interest (b). The Old Directive already provided for an override of the elimination of caller identification on a per-line basis for organizations dealing with emergency calls and recognized as such by Member States. The Directive does not change this option for an override in the public interest. The requirement of recognition by a Member State shows that the organization has to be a professional body specialized in dealing with emergency calls. Law enforcement agencies (i.e., the police), ambulance services and fire brigades are mentioned as examples. Organizations which occasionally receive emergency calls while carrying out different functions will not qualify for a public interest override. The Directive also takes into account the new art. 9 on location data. Although it mentions only 'location data' without referring to art. 9, the wording of art. 10(b) obviously refers to art. 9(2). It allows for the processing of location data other than traffic data where users or subscribers have exercised their right under art. 9(2) to refuse temporarily the processing of these data for a connection to the network or for a transmission of communication. The underlying rationale here again is the need to locate a person in an emergency situation by using location data for value added services which are more precise than traffic data (which may also include location information relevant for billing purposes). This exception only applies in situations where location data have been processed with the initial informed consent of the users or subscribers according to art. 9(1) for if no location data are processed in the first place they cannot be generated without the consent of the data subject (user or subscriber). There is therefore a difference between the eliminated presentation of calling line identification and the temporary denial or absence of consent for the processing of location data: if the presentation of calling line identification is offered, presentation is the default situation (it needs no additional consent) and users or subscribers have to make a choice whether they want to increase their privacy by eliminating calling line identification. However, if value added services on the basis of location data are offered, users or subscribers may accept this offer and give their consent to the processing of location data or they may refuse to do so. The default situation here (without initial consent) is that no location data are processed. Only if consent to the processing of location data has initially been given (to use value added location based services) and later has been temporarily withdrawn will the exception of art. 10(b) come into play. The location data registered before consent was withdrawn may under these circumstances be used. The only legal purpose for the override is to respond (or rather: react) to emergency calls. This purpose limitation is particularly important for law enforcement agencies which are organizations receiving and dealing with emergency calls. The override function may not be used for the general purpose of law enforcement (quite apart from the fact that these matters cannot be dealt with in a Directive based on the First Pillar (internal market) provisions of Community Law).

[Automatic call forwarding]

Article 11

Member States shall ensure that any subscriber has the possibility, using a simple means and free of charge, of stopping automatic call forwarding by a third party to the subscriber's terminal.

General. Automatic call forwarding is the possibility offered for the benefit of the users to instruct the network to forward calls to another terminal equipment. This service will permit users absent from their domicile to forward calls from their telephony terminal equipment to other telephony equipment or to their mobiles. Insofar as the definition of 'call' under art. 2(e) refers only to voice telephony services, the provision is not applicable to internet services consisting in redirecting e-mail or request to a website to another place as well, through visible or invisible hyperlinks. Perhaps, as regards these services not covered by the Directive, it might be emphasised that technical user-friendly solutions might be easily given in this new context through available filtering options, for example, in the e-mail programme itself or through the blocking of automatic hyperlinks. The provision laid down under art. 11 requires that the subscriber to whom the call has been redirected have the possibility to stop the automatic call forwarding decided by a third party through 'simple means and free of charge'. The text restates the similar provision contained in the old 1997 Directive.

[Directories of subscribers]

Article 12

(1) Member States shall ensure that subscribers are informed, free of charge and before they are included in the directory, about the purpose(s) of a printed or electronic directory of subscribers available to the public or obtainable through directory enquiry services, in which their personal data can be included and o any further usage possibilities based on search functions embedded in electronic versions of the directory.

(2) Member States shall ensure that subscribers are given the opportunity to determine whether their personal data are included in a public directory, and if so, which, to the extent that such data are relevant for the purpose of the directory as determined by the provider of the directory, and to verify, correct or withdraw such data. Not being included in a public subscriber directory, verifying, correcting or withdrawing personal data from it shall be free of charge.

(3) Member States may require that for any purpose of a public directory other than the search of contact details of persons on the basis of their name and, where necessary, a minimum of other identifiers, additional consent be asked of the subscribers.

(4) Paragraphs 1 and 2 shall apply to subscribers who are natural persons. Member States shall ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to their entry in public directories are sufficiently protected.

1. General. The structure and the wording of art. 12 differ considerably from its predecessor (art. 11) in the Old Directive. The object of both provisions is to guarantee the data subject's informational autonomy with regard to directory services. This is to be seen against the background of the telecom monopolies before liberalization of the European telecommunications markets in the 1990s. Monopolist carriers or providers in many Member States published directories and offered directory enquiry services without offering the data subjects any options as to the inclusion of their personal data in these directories and services. There were no legal limits as to the extent to which personal data were included in these directories or services. Therefore the Old Directive for the first time stated that personal data contained in printed or electronic directories of subscribers available to the public should be limited to what is necessary to identify subscribers unless they had consented to the publication of additional personal data. Subscribers were given the right to be omitted from the directory altogether, to limit the amount of data included in the directory and to indicate that the data may not be used for direct marketing purposes. Art. 12 clarifies these rights and strengthens the position of the subscribers in a number of respects. The principle that only personal data which are necessary to identify the data subject should be included in the directory is no longer mentioned in art. 12 since this follows from the Data Protection Directive (See commentary on art. 1(2)).

2. Right to information (para. 1). The Directive rightly emphasizes the subscriber's right to thorough information before any of that subscriber's data are included in a printed or electronic directory. In addition subscribers have to be informed of the purpose(s) of a publicly available printed or electronic directory. This is of particular importance in the digital era since electronic enquiry services rely on powerful databases where the software supports numerous search functions (e.g., reverse searching, see Working Paper 33). Reverse searching allows for the finding out of the name and possibly the address of the subscriber simply by means of the telephone number or the names and telephone numbers of all people living in the same street by means of the street name. As the Working Party has put it: 'It is possible to learn much more about an individual than he or she would imagine when accepting to have his or her telephone number in the directory.' An itemized bill with telephone numbers of called persons could be used to produce an entire list with names and addresses of all persons called by one particular subscriber. Other search facilities may include location information. Electronic telephone directories may be analyzed with data mining or data warehousing tools. Also directory data may have to be transmitted to third parties under universal service obligations (see art. 6 of the Universal Service Directive and the KPN (ECJ) judgment) and may be published online or in offline media (e.g., CD-ROM, DVD). These further uses reduce data subjects' chances to control the processing of their personal data once these have been included in a printed or electronic directory. Even printed directories may be scanned or otherwise turned into electronic versions. Once directories are published it is difficult to prevent their use for purposes other than the original purpose for which they have been collected (e.g., direct marketing). Therefore complete information for subscribers is a necessary prerequisite for them to make informed choices according to paras. 2 and 3. The Directive, when referring to 'purpose(s)', envisages that directories may have more than one purpose and these may be purposes which go beyond the mere identification of a subscriber. New products and business models are conceivable and legal as long as their purpose is made completely transparent to the data subjects. The duty to inform the subscriber lies with the party (provider) collecting the data for inclusion in a directory or database (see recital 39).

3. Subscribers' privacy options (para. 2). With the necessary information according to para. 1 in hand, subscribers are in a position to exercise their privacy options. Firstly, they have the right to stay out of any telephone directory altogether. No charge may be raised if they choose to do so. This is an improvement in relation to the Old Directive where in exceptional cases a limited payment could be asked for. Also subscribers do not have to give reasons for their choice. If subscribers choose to have personal data included in the directory they may limit the inclusion to specific data. They may also opt for the inclusion of additional data as long as these data are 'relevant for the purpose of the directory as determined by the provider'. Here again the Directive makes it clear that it is for the provider to determine the purpose of the directory or enquiry service which it is offering. Data subjects, after having been informed of this purpose (see para. 1), can then decide if they want to have their personal data included in such a directory or database. Furthermore subscribers have the right at any time and without charge or having to give reasons to withdraw their consent and to have their data removed from the directory or database. This will encounter practical problems in printed directories which have been published; the withdrawal will only take effect in later printed versions of the directory. Indeed it may not become completely effective at all since old versions of the directory may have been sold or scanned by third parties. Although the Directive does not say so explicitly Member States are well advised to oblige providers of directory services (esp. those under universal service obligations) who receive the request for withdrawal from a subscriber to inform those third parties to whom they have transmitted the data in the meantime that the subscriber has withdrawn consent. Although the Directive does not legally bind them to do so, Member States should also ensure that subscribers can limit the

publication of their data to printed directories and exclude their integration in electronic databases. If the entry into the printed directory included a mark (e.g., asterisk), documenting the subscriber's preference digital copies of such a printed directory could either be made without these data or, if the subscriber's preference was not taken into account, the author of the digital copy could be held liable.

4. Opt-in for reverse searching (para. 3). Since reverse searching facilities change the purpose and the possible use of an electronic directory (see commentary para. 2 above) the Directive enables Member States to require additional opt-in of subscribers. If it does not require such an opt-in, an opt-out would equally be in line with the Directive. Indeed, one could argue that in the digital era it is hard to prevent individual users of directory services to reverse databases which they bought on offline media (CD-ROM, DVD) with their own hard and software. But at any rate the providers of directory services collecting data are obliged to inform subscribers of any opt-in or opt-out option they offer with regard to reverse searching facilities.

5. Extension to legal persons (para. 4). Although paras. 1 and 2 primarily apply to natural persons, Member States are called upon to ensure the sufficient protection of legitimate interests of legal persons with regard to their entry in public directories. Neither the notions of legitimate interests of legal persons nor 'sufficient protection' are defined in the Directive (See Commentary on art. 1(2)). There is no obligation under Community Law to extend the protection afforded by the Data Protection Directive to legal persons (see recital 12). Even if Member States provide for a certain degree of protection of legal persons it may be different and at a lower level than the protection provided for natural persons under the Directive.

[Unsolicited communications]

Article 13

(1) The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent.

(2) Notwithstanding paragraph 1, where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use.

Directive 2002/58/EC, art. 13

(3) Member States shall take appropriate measures to ensure that, free of charge, unsolicited communications for purposes of direct marketing, in cases other than those referred to in paragraphs 1 and 2, are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these communications, the choice between these options to be determined by national legislation.

(4) In any event, the practice of sending electronic mail for purposes of direct marketing disguising or concealing the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease, shall be prohibited.

(5) Paragraphs 1 and 3 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected.

1. General. (a) Legal framework. This article relates to the sending of unsolicited communications. This is not the only text regulating the sending of unsolicited communication. The Directive on distance marketing of consumer financial services, the Directive on distance contracts, the Directive on electronic commerce as well as the Data Protection Directive also define specific conditions with regard to the sending of unsolicited communications for commercial or for direct marketing purposes. These directives remain applicable to the matter, in particular with respect to recipients who are not affected by the provisions of art. 13. The Directive also expressly states in recital 45 that where Member States establish an opt-out register for unsolicited communications to legal persons, the provisions of the Directive on electronic commerce remain fully applicable. The Old Directive also contained a specific provision with respect to unsolicited communications. The Directive, however, innovates in this regard. First, it extends the application of the opt-in rule to the use of electronic mail for direct marketing purposes. Second, the Directive creates an exemption regime, that is, the 'soft opt-in' rule in the context of an existing customer relationship between a client and a supplier. Finally, the Directive strengthens the protection afforded recipients of direct marketing communications by introducing specific rules with respect to the self-identification of the sender of unsolicited communications. **(b) Extraterritorial aspects.** As mentioned in commentary on art. 3(1), the criteria determining the territorial scope of application of the Directive differ from those defined in art. 4 of the Data Protection Directive. Therefore, the Directive binds controllers who are processing personal data in the context of the activities of an establishment which is not located on the European Community territory. Art. 13 thus applies to data controllers who are established outside the European Community territory as

soon as they are sending unsolicited communications to persons established on this territory.

2. Use of automated calling systems without human intervention, facsimile machines or electronic mail automated means (para. 1). (a) Use of automated means. Art. 13 distinguishes between the sending of unsolicited communications via the use of automated calling systems without human intervention, facsimile machines or electronic mail automated means ruled in para. 1 and the use for other means, such as person-to-person telephony calls governed by para. 3. Recitals 40 and 42 explain this differentiation by the fact that, contrary to other forms of direct marketing, the sending of unsolicited communications by such automated means such is relatively easy and cheap and may impose a burden and/or cost on the recipient and the volume of communications may cause difficulties for electronic communications networks and terminal equipment. **(b) Opt-in rule.** *Consent.* Para. 1 regulates the use of automated calling systems without human intervention such as automatic calling machines, facsimile machines or electronic mail (see definition in commentary on art. 2(2)(h)) for the purposes of direct marketing. Such use can only be allowed for the purpose of sending this kind of unsolicited communications to subscribers who have given their prior consent in this regard. In order to be valid, the consent needs to respect the requirements of the Data Protection Directive, that is to be informed, specific and freely given. This rule raises a practical issue: the mere fact of contacting recipients to ask them whether they would consent to receiving unsolicited material has been considered as already constituting an electronic mail for marketing purpose. This is a major issue when the sender has gathered information of potential recipients under an opt-out regime and wishes to continue to use the list for direct marketing purposes under the opt-in rule introduced by the Directive (Opinion on unsolicited communications, p. 6). *Prior information.* The consent must be preceded by the provision of the information required by the Data Protection Directive (see comment on art. 2(2)(f) with respect of the concept of 'consent'). *Modalities of the obtaining of the consent.* The Working Party points out that it would not be compatible with art. 13 simply to ask, by a general e-mail sent to recipients, their consent to receive marketing e-mails, because of the requirement that the purpose be legitimate, explicit and specific. Moreover, the Working Party also excludes any form of implied consent including consent that may be assumed unless objection is made, such as through the use of pre-ticked boxes. Nevertheless, methods whereby subscribers give prior consent by registering on a website and who are later asked to confirm that they were the ones who registered and to confirm consent are in compliance with the Directive (Opinion on unsolicited communications, p. 5; see also comment on definition of the term 'consent' in art. 2(2)(f)). **(c) Senders bound by the opt-in rule.** The persons addressed by this rule are not limited to the providers of publicly available electronic communications or the provider of a public communications network. Para. 1 prohibits the use of certain automatic means for the purpose of sending unsolicited communication regardless of the type of sender. **(d) Persons protected.** Despite the fact that para. 1 refers to subscribers without excluding subscribers who are legal persons, para. 5 states that para. 1 only applies to subscribers who are natural persons. It is also remarkable that this provision only addresses 'subscribers' and not 'users' of a publicly available electronic communications service. This implies, for instance, that the sending of unsolicited communications to employees or family members who are not the subscribers but only the users of an electronic communications service is not governed by para. 1. The consequences of the requirement of the consent by the subscriber alone are not very clear. Does it imply that the sending of unsolicited communications for direct marketing purposes to users who are not subscribers is not subject to any conditions under the Directive and is only subject to rules defined in other directives or that it will be subordinated to the consent of the subscriber to the service? In such a case, the rule could vary depending on the fact that the subscriber is a natural person (opt-in rule) or a legal person (rule to be determined by national law – see commentary on para. 5). In order to assess whether the opt-in rule applies, the sender will then not only need to determine whether the recipient is a legal or a natural person but also whether it is a subscriber or a user. **(e) Concept of direct marketing.** The Directive does not provide for any definition of the terms 'direct marketing'. The Working Party, however, considers that art. 13 not only relates to communication of a pure commercial nature but also covers any form of sales promotion, including direct marketing by charities and political organizations such as fund raising, and so forth. Newsletters sent by e-mail also fall under the scope of this definition (Opinion on unsolicited communications, pp. 4 and 7).

3. 'Soft opt-in' for the use of electronic mail in customer relationships (para. 2). (a) The 'soft opt-in' concept. Para. 2 introduces an exception to the opt-in rule defined in para. 1 for the use of electronic contact details for electronic mail in a customer relationship between the sender and the recipient. Subject to certain conditions, the opt-out rule replaces the opt-in rule in such a context. The opt-out rule means that the recipient will be entitled to oppose to the use of its contact details for e-mailing of direct marketing content but will not be required to give its prior consent for such use. Since the benefit of this exception is subject to several cumulative conditions, including the existence of a prior customer relationship, this regime is generally called 'soft opt-in'. **(b) Conditions for 'soft opt-in'.** Firstly, the contact details for electronic mail must have been obtained by the sender from its customer and not from a third party. Second, these data must have been collected in the context of the sale of a product or a service. Third, they must have been collected in accordance with the provisions of the Data Protection Directive, which includes complying with the requirement of information of the data subjects regarding the purpose of direct marketing and the respect of the data subjects' right to oppose to such use. Para. 2 expressly indicates that the customers must clearly and distinctly

have been given the opportunity to object, free of charge and without difficulty, to such use of electronic contact details when they have been collected. In addition to these conditions, para. 2 limits the use that can be further made of the electronic contact details: only the natural or the legal person who collected the contact details can use these data. For instance, they could not be used by other companies of the group to which the company that collected the data pertains. Moreover, the use of these data will only be possible for direct marketing of the sender's own similar products or services. The Working Party indicated that such similarity should be judged on an objective basis, that is, the reasonable expectations of the recipient, rather than from the perspective of the sender (Opinion on unsolicited communications, p. 9). Finally, the sender must, at the occasion of each direct marketing message sent, give clearly and distinctly the opportunity to the customer to object, free of charge and without difficulty, to such use of electronic contact details in the event the customer has not initially refused such use. **(c) Beneficiaries of the soft opt-in rule.** Para. 2 has a broad application since it addresses any natural or legal person who provides products or services. **(d) Persons protected.** Para. 2 uses the term 'customer' to identify the recipients concerned by this exemption. Since para. 1 appears only to protect natural persons who are subscribers, it would be reasonable to consider that the exception to the regime defined under para. 1 also targets the same category of recipients.

4. Use of other means (para. 3). (a) Choice between opt-in and opt-out. Para. 3 relates to cases other than those referred to in paras. 1 and 2. The European Commission expressed the view that pop-up messages fall under the scope of para. 3 (Answer to written question E-3392/02, 2003/C 155 E/164). Pursuant to para. 3, Member States will have the possibility of subjecting the use of means other than automated calling systems without human intervention, facsimile machines or electronic mail for direct marketing purpose either to the opt-in or to the opt-out rule. Member States will indeed have to take appropriate measures to ensure that, free of charge, unsolicited communications for purposes of direct marketing are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these communications. The choice between these options is, therefore, to be determined by national legislation. This will allow the Member States which had implemented an opt-in regime to the use of this communications prior to the Directive to maintain this level of protection. **(b) Senders concerned by para. 3.** The persons addressed by this paragraph are not limited to the provider of publicly available electronic communications or the provider of a public communications network since para. 3 governs the use of the non-automated means for the purpose of sending unsolicited communication regardless of the quality of the sender. **(c) Persons protected.** Pursuant to para. 5, para. 1 only applies to subscribers who are natural persons. Furthermore, like para. 1, para. 3 relates to data subjects who are 'subscribers' and not to the 'users' of a publicly available electronic communications service.

5. Prohibition of the use of false identity or invalid addresses (para. 4). Para. 4 defines additional requirements applying to the use of electronic mail for purposes of direct marketing regardless of the quality of the recipient (subscriber, user, natural or legal person). Para. 4 prohibits the practice of disguising or concealing the identity of the sender of the electronic mail on whose behalf the communication is made. It also imposes the use of a valid address or number to which the recipient may send a request that such communications cease. As explained by recital 43, these additional requirements are necessary to ensure the effective enforcement of the above-mentioned rules or of rules defined in other European directives on unsolicited messages for direct marketing. The use of false identities or false return addresses or numbers would indeed impede the data subjects to enforce their rights, in particular the right to opt-out.

6. Protection of legal person's interests (para 5). As mentioned in the commentary on paras. 1 and 3, para. 5 specifies that the rules defined in these two paragraphs apply to subscribers who are natural persons. With regard to subscribers who are legal persons, para. 5 requires the Member States to ensure, in the framework of Community law and applicable national legislation, that their legitimate interests are sufficiently protected. This provision leaves a great freedom to the Member States since it does not provide for any recommendation as to the concrete measures that need to be implemented (opt-in, opt-out or others) or as to the level protection that should be afforded to subscribers who are legal persons pursuant to the protection of their 'legitimate interests'. The Working Party noticed in that respect that the implementation of this provision will raise different pragmatic issues. Firstly, it might not always be easy to identify whether the recipient is a legal or a natural person and it is not clear what efforts can be expected from a sender to verify whether the address or number belongs to a legal or a natural person. Moreover, it is likely that discrepancies between national legislations will arise and it is not clear how cross-border effects will be dealt with if the rule that applies to electronic mail originating in a Member State differs from the one that applies in the Member States where the electronic mail is received (Opinion on unsolicited communications, p. 8).

[Technical features and standardisation]

Article 14

(1) In implementing the provisions of this Directive, Member States shall ensure, subject to paragraphs 2 and 3, that no mandatory requirements for specific technical features are imposed on terminal or other electronic communication equipment which could impede the placing of equipment on the market and the free circulation of such equipment in and between Member States.

(2) Where provisions of this Directive can be implemented only by requiring specific technical features in electronic communications networks, Member

States shall inform the Commission in accordance with the procedure provided for by Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on information society services (Directive as amended by Directive 98/48/EC (OJ L 217/18, 5 August 1998), OJ L 204/37, 21 July 1998).

(3) Where required, measures may be adopted to ensure that terminal equipment is constructed in a way that is compatible with the right of users to protect and control the use of their personal data, in accordance with Directive 1999/5/EC and Council Decision 87/95/EEC of 22 December 1986 on standardisation in the field of information technology and communications (Decision as last amended by the 1994 Act of Accession, OJ L 36/31, 7 February 1987).

1. Regulatory objective. The Directive provides for a regulatory framework which is basically technology neutral. Thus the European regulator is unlikely to face a situation in the near future where there is a need to redraft the Directive due to fundamental technological changes. However, in order to prevent negative effects on the single market Member States are either required to abstain from any regulatory requirements for terminal equipment which may inhibit free circulation of such products or to inform the Commission about specific requirements for networks. But the Directive allows for national regulations and standardization of privacy-enhancing terminal equipment.

2. Technical requirements for equipment (para. 1). It is an important objective of the European Community to create a single and competitive market for telecommunications services as well as for terminal equipment. The Directive therefore stresses that Member States – when implementing the provisions of the Directive – should ensure that no requirements for specific technical features are imposed on terminal equipment or other electronic communication equipment if such requirements could prevent this equipment from being placed on the single market or from circulating there. Requirements which do not influence the introduction in the market or the free circulation in the Community can be imposed without infringing the Directive. It is somewhat unclear what is meant by 'other electronic communication equipment'. The provision seems to refer to any hardor software component which is not a terminal. However, since para. 2 deals with networks and para. 3 with terminal equipment exclusively the 'equipment' to which para. 1 refers cannot include network infrastructure such as routers.

3. Technical requirements for networks (para. 2). If provisions of the Directive can only be implemented by requiring specific technical features in electronic communications networks, the Directive requires Member States to inform the Commission in accordance with Directive 98/34/EC. This Directive provides for a procedure to achieve transparency as well as uniformity in the field of standardization in the Member States. Once

a Member State has informed the Commission of a draft technical standard the adoption of this draft has to be postponed for a standstill period of up to twelve months if the Commission either announces its intention to propose or adopt legislation in the field where the Member State plans to adopt a national draft technical regulation or the Commission finds that this draft technical regulation is covered by existing Community legislation. The objective is to support harmonization of technical standards in the Community. By referring to Directive 98/34/EC, art. 14(2) prevents further diversity in this field which would inhibit the single telecommunications market. At least the Member States cannot adopt technical regulations in this field before the Commission has been informed and had a chance to initiate Europe-wide regulation.

4. Privacy-enhancing terminal equipment (para. 3). In a somewhat erratic fashion para. 3 returns to requirements for terminal equipment (which has already been dealt with inter alia in para. 1). The Directive acknowledges that technology may be compatible or incompatible with the right of users to protect and control the use of their data. Therefore the implementation of the Directive may not be entirely technology neutral. Member States may – where necessary – adopt measures which ensure that terminal equipment ('other electronic communication equipment' – in contrast to para. 1 – is not mentioned here) is compatible with the rights of users under the Directive. Indeed, measures which require privacy-enhancing features in terminal equipment (e.g., a simple means to eliminate calling line identification according to art. 8) may be vital for the successful implementation of the Directive. If Member States adopt such measure they have to take into account the R & TTE-Directive as well as the Council Decision of 1986 on standardization in this field. Here again the implementation of the Directive has to be reconciled with the requirements of Europe-wide conformity and standardization of terminal equipment. It is all the more important that European standards on privacy-enhancing telecommunications terminal equipment are proposed and implemented (see recital 46). This would lead to technological support for the data protection rights of users and would prevent divergent national requirements with regard to technical specification.

[Application of certain provisions of Directive 95/46/EC]

Article 15

(1) Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8 (1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the communications system, as referred to in Article 13(1) of the Directive 95/46/EC. To this end, Member States may, inter alia,

adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6 (1) and (2) of the Treaty on European Union.

(2) The provisions of Chapter III on judicial remedies, liability and sanctions of Directive 95/46/EC shall apply with regard to national provisions adopted pursuant to this Directive and with regard to the individual rights derived from this Directive.

(3) The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC shall also carry out the tasks laid down in Article 30 of that Directive with regard to matters covered by this Directive namely the protection of fundamental rights and freedoms and of legitimate interests in the electronic communications sector.

1. Regulatory objective. The provision explains in some detail under which conditions certain rights flowing from the Directive may be restricted, and how specific provisions of the Data Protection Directive are to be applied in the context of this Directive.

2. Restrictions on certain rights (para. 1). As is explicitly stated in recital 11 the Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law (the so-called Third Pillar, namely, inter-governmental cooperation in matters of Justice and Internal Affairs). Nevertheless, the authors of the Directive felt the need to address these issues albeit for the sake of clarification. They had no legal basis in this Directive to regulate matters falling within the scope of the Third Pillar since this Directive was passed by the European Parliament and the Council whereas a Third Pillar measure would have required a unanimous vote in the Council and no participation or co-decision from the European Parliament. Therefore art. 15 (1) (like the equivalent provision of art. 13 of the Data Protection Directive) has a merely declaratory function to state that these Directives do not restrict the powers of Member States to act in a specific way once issues of national or public security are at stake. Nevertheless, Member States cannot rely on these Directives to claim legal authority for such measures or even to an obligation to take such measures under European Law. Such proposals (e.g., for routine retention of traffic data) are at present under discussion but have not yet been passed. The exceptional restrictions explained in this provision do not apply to the entire Directive but only to Articles 5 (Confidentiality of electronic communications), 6 (Processing of traffic data), 8 (paras. 1-4) (Presentation and restriction of calling and connected line identification) and 9 (Processing of location data). The other provisions of the Directive containing rights of individual users (especially art. 5, Security, art. 7 Itemized billing, art. 11, Automatic call forwarding, art. 12, Directories of subscribers, and art. 13, Unsolicited

communications, are not subject to the restrictions mentioned in art. 15(1)). Although art. 15(1) explicitly refers to the equivalent exception in the Data Protection Directive (art. 13) it differs considerably from this provision in that it uses language which is much closer to the famous wording of the European Convention of Human Rights (see arts. 8(2) and 10(2) of the Convention). Whereas art. 15(2) only allows for restrictions which constitute 'a necessary, appropriate and proportionate measure within a democratic society', the Data Protection Directive merely speaks of 'necessary measures'. The explicit emphasis on the European standard for the protection of human rights has notably increased with the adoption of the present Directive. In the meantime, however, the European Court of Justice has in turn interpreted the Data Protection Directive on two occasions with reference to the European Convention and to the fundamental rights protected by the Community legal order (see *Österreichischer Rundfunk* (ECJ); *Bodil Lindqvist* (ECJ)). The list of exceptional circumstances in this Directive is also shorter and more general when compared with the Data Protection Directive. National security (paraphrased as 'State security'), defence, public security and the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the electronic communications system are the only legitimate purposes to restricting certain rights under the Directive. Other exceptions such as economic or fiscal interests of Member States or breaches of ethics for regulated professions (see art. 13(1)(d),(e)) Data Protection Directive) do not justify restrictive measures in electronic communications. The most important case in practice of a right to be restricted in such circumstances is the right to communicate confidentially if a telephone conversation or e-mail communication is overheard or tapped by law enforcement agencies. With its reference to the European Convention of Human Rights as well as to art. 6(1) and (2) of the Treaty of the European Union the Directive at the same time makes reference to the extensive case law of the European Court of Human Rights (see recital 11) on issues such as telephone tapping. When adopting measures to restrict rights under the Directive (art. 6 in particular) Member States have to take into account the principles of this case law. With regard to data retention the Directive allows inter alia for the adoption by Member States of legislative measures providing for the retention of data for a limited period justified on the grounds mentioned above. It is doubtful whether this wording includes the routine retention of all traffic data generated in telecommunications networks even before any particular threat to national security has occurred or any crime has been committed for the prosecution of which the analysis of certain traffic data might be necessary. Furthermore the European Court of Human Rights has on numerous occasions stressed that there must be a 'pressing social need' before a measure can be deemed to be necessary in a democratic society; the mere usefulness for purposes of crime prevention or detection is not sufficient to justify restrictions of fundamental rights (see the *Klass* judgment (ECHR)). It is very doubtful if routine retention of traffic data can be considered

a necessary and proportionate measure in this sense since there are other measures available such as data preservation orders ('fast freeze – quick thaw') preventing the erasure of existing traffic data once a particular crime has been committed or a specific danger is imminent (see Working Paper 99). In view of the case law both of the European Court of Human Rights and the European Court of Justice it is scarcely conceivable that any measure requiring the routine and systematic retention of traffic data for general purposes of crime prevention or detection would be upheld by these courts.

3. Judicial remedies (para. 2). Whereas art. 1(2) underlines in general the complementary character of the Directive in relation to the Data Protection Directive, art. 15(2) explicitly declares applicable Chapter III (arts. 22-24) of the Data Protection Directive with regard to national laws implementing the Directive and to the individual rights conferred by the Directive. It is important that Member States provide for judicial remedies, liabilities and sanctions when implementing the Directive (see recital 47). Market mechanisms alone will not ensure that rights of users and subscribers in the sphere of electronic communications are respected.

4. Working Party (para. 3). At some stage during the discussions on the draft for the Old Directive it was argued that a separate Working Party should be established to oversee the application of the Directive and advise the Commission in this era. However, the Old Directive and the present Directive ultimately adopted the comitology of the Data Protection Directive by entrusting the tasks under art. 30 of that Directive to the existing Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of the Data Protection Directive. This is in line with the material reference made in art. 1(2) of the Directive on Electronic Communications: if this Directive complements the Data Protection Directive and the two legislative measures have to be read together then it makes sense to have one Working Party including the supervisory authorities from all Member States overseeing the application of both Directives and advising the Commission in both fields. The Working Party has already adopted numerous opinions dealing with questions of electronic communications (see esp. Working Papers 18, 25, 29, 33, 36, 57, 58, 64, 76 and 99).

[Transitional arrangements]

Article 16

(1) Article 12 shall not apply to editions of directories already produced or placed on the market in printed or off-line electronic form before the national provisions adopted pursuant to this Directive enter into force.

(2) Where the personal data of subscribers to fixed or mobile public voice telephony services have been included in a public subscriber directory in

conformity with the provisions of Directive 95/46/EC and of Article 11 of Directive 97/66/EC before the national provisions adopted in pursuance of this Directive enter into force, the personal data of such subscribers may remain included in this public directory in its printed or electronic versions, including versions with reverse search functions, unless subscribers indicate otherwise, after having received complete information about purposes and options in accordance with Article 12 of this Directive.

(1) General. The Directive includes transitional provisions for subscriber directories according to art. 12 in two sets of cases: editions directories which have been produced before the Directive has been implemented in the Member States and directories which include subscriber data in conformity with the Data Protection Directive and the Old Directive.

(2) Off-line Directories produced before implementation of the Directive (para. 1). Where directories have been printed or produced in off-line electronic versions before the national provisions implementing the Directive enter into force, the Directive will not apply. It does apply to on-line electronic versions of such directories since they can easily be adapted to the new legal regime. Art. 12 will also apply to the next edition after the entry into force of national provisions implementing the Directive.

(3) Voice telephony directories produced before implementation (para. 2). Where public directories of subscribers to public voice telephony services have been published (on-line, printed or electronic off-line) including subscriber data in accordance with the Data Protection Directive and art. 11 of the Old Directive before national provisions implementing the Directive enter into force then the data will remain included in these directories until a subscriber, after being fully informed (see art. 12(1)), opts out. This applies also to electronic versions including reverse search facilities. In practice this means that the opt-in solution provided for in art. 12 becomes an opt-out solution in the majority of cases (existing directories of voice telephony subscribers).

[Transposition]

Article 17

(1) Before 31 October 2003 Member States shall bring force the provisions necessary to comply with this Directive. They shall forthwith inform the Commission thereof. When Member States adopt those provisions, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.

(2) Member States shall communicate to the Commission the text of the provisions of national law which they adopt in the field governed by this Directive and of any subsequent amendments to those provisions.

[Review]

Article 18

The Commission shall submit to the European Parliament and the Council, not later than three years after the date referred to in Article 17(1), a report on the application of this Directive and its impact on economic operators and consumers, in particular as regards the provisions on unsolicited communications, taking into account the international environment. For this purpose, the Commission may request information from the Member States, which shall be supplied without undue delay. Where appropriate, the Commission shall submit proposals to amend this Directive, taking account of the results of that report, any changes in the sector and any other proposal it may deem necessary in order to improve the effectiveness of this Directive.

[Repeal]

Article 19

Directive 97/66/EC is hereby repealed with effect from the date referred to in Article 17(1). References made to the repealed Directive shall be construed as being made to this Directive.

[Entry into force]

Article 20

This Directive shall enter into force on the day of its publication in the Official Journal of the European Communities.

[Addressees]

Article 21

This Directive is addressed to the Member States.